日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９７年１０月　１日

出願番号
Application Number: 平成　９年特許願第２６８８９１号

出願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９７年１２月１９日

特許庁長官
Commissioner,
Patent Office

荒井寿光

【書類名】　特許願

【整理番号】　9704230

【提出日】　平成 9年10月 1日

【あて先】　特許庁長官殿

【国際特許分類】　G07F　7/08

G06F 15/30

G06K 17/00

【発明の名称】　二重財布を有する電子財布システム、その電子財布システムに適用されるＩＣカード、二重財布を有するＩＣカード取引装置、二重財布を有するＩＣカード取引システムおよびそのＩＣカード取引システムに適用されるＩＣカード

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　西尾　信彦

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　麻生　泉

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　二重財布を有する電子財布システム、その電子財布システムに適用されるＩＣカード、二重財布を有するＩＣカード取引装置、二重財布を有するＩＣカード取引システムおよびそのＩＣカード取引システムに適用されるＩＣカード

【特許請求の範囲】

【請求項１】　第１預金額が格納される第１領域と第２預金額が格納される第２領域とを備えた書き換え可能な第１不揮発性メモリと、当該メモリに接続された処理装置と、当該処理装置の動作プログラムを格納した第２不揮発性メモリと、当該処理装置を介して前記第１，第２不揮発性メモリにそれぞれ格納された情報にアクセスするための入力端子を備えた携帯型のカード状担体であって、

前記第１不揮発性メモリの第１領域に対応して少なくともカード所有者の個人認証番号が前記第１不揮発性メモリに格納され、

前記第１不揮発性メモリの第２領域に対応して当該第２領域へのアクセスを許容できる装置の種類を示す識別情報が前記第１不揮発性メモリに格納され、

前記第１領域へのアクセスに際して前記入出力端子から入力され暗号化された情報を解読し、その解読された情報に含まれる暗証番号と前記第１不揮発性メモリに格納された個人認証番号とが所定の関係である場合にアクセスを許容し、

前記第２領域へのアクセスに際してアクセスする取引装置の種類を示す識別番号が一致する場合、前記第２領域へのアクセスを許容するカード状担体と、

預金額が格納された口座ファイルを有するセンタシステムと、

前記カード状担体のメモリの第１領域に、前記センタシステムの預金額の一部または全部を移送するための前記センタシステムに直接または間接的に連携された引出装置であって、

装置の識別情報と、カード所有者が入力した暗証番号の内、少なくとも一方を暗号化して前記カード状担体に転送する引出装置と、

暗証番号および前記カード状担体における前記第１領域から前記第２領域に転送すべき金額を入力する入力手段と、前記カード状担体に対して前記入力手段によって入力された暗証番号と転送金額と識別情報とを供給する転送装置と、

前記カード状担体の第２領域に格納された預金額を使用するため、利用金額と装置情報とを送出する利用装置と、

を備え、

前記カード状担体は、

前記転送装置によって転送を指示され、かつ前記個人認証番号が許容された場合には、前記第１領域に格納された預金額を指定された金額分減算して前記第１領域の更新を行うとともに、前記第２領域に指定された金額を書き込み、

前記利用装置により利用金額を指示され、かつ前記識別情報が前記第２領域へのアクセスを許容された場合には、前記利用金額を減算して前記利用装置での前記利用金額の利用を許容することを特徴とする二重財布を有する電子財布システム。

【請求項２】　前記カード状担体は、前記第２不揮発性メモリに前記第２領域が引出処理のみ許容するプログラムを格納していることを特徴とする請求項１に記載の二重財布を有する電子財布システム。

【請求項３】　前記カード状担体は、前記第１不揮発性メモリに第３領域を有し、前記第３領域には、当該第３領域へのアクセスを許容する利用装置の識別情報および暗証番号が登録され、前記第２不揮発性メモリには、前記利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に前記第３領域の加算又は減算を許容するプログラムが格納されていることを特徴とする請求項１に記載の電子財布システム。

【請求項４】　前記カード状担体は、前記第３領域に、加算処理した前記利用装置を示す識別情報と加算処理した額とを履歴情報として格納することを特徴とする請求項３に記載の二重財布を有する電子財布システム。

【請求項５】　前記カード状担体は、前記利用装置が前記第１不揮発性メモリの領域を指定せずに支払い処理を要求した際に、前記利用装置からの転送情報の復号化処理をスキップして、前記第２預金額から指定された金額情報を差し引く取引きを許容することを特徴とする請求項２に記載の二重財布を有する電子財布システム。

【請求項６】　第１金額が記憶された第１財布、第２金額が記憶された第２

財布、支払い処理プログラム、利用者の暗証番号プログラムを格納したメモリと、

前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、

外部装置と通信を遂行する通信手段と、

を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって、

前記支払いプログラムは、

外部の支払い要求装置から、財布を指定せずに支払いコマンドを受信した場合、前記第２財布に格納された第２金額に基づき支払い処理し、前記第１財布を指定した支払いコマンドを受信した場合、暗証照合を行い、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする二重財布を有する電子財布システムに適用されるＩＣカード。

【請求項７】　第１金額が記憶された第１財布、第２金額が記憶された第２財布、支払い処理プログラムおよび暗号化／復号化プログラムを格納したメモリと、

前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、

外部装置と通信を遂行する通信手段と、

外部の取引装置とのインタフェースを司るインタフェース手段と、

を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって、

前記支払いプログラムは、

前記インタフェース手段を通じて外部装置から第１財布を指定せずにコマンドを受信した場合、前記第２財布に格納された第２金額に基づいて支払い処理を遂行し、前記第１財布を指定した支払いコマンドを受信した場合、前記暗号化および復号化プログラムを使用して、外部の装置と通信し、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする二重財布を有する電子財布システムに適用されるＩＣカード。

【請求項８】　ＩＣカードに格納される金額とセンタ口座に格納される金額との内の一方を選択し、その選択された金額に基づいて現金支払いを行うＩＣカード取引装置であって、

ＩＣカードの装着を検出する検出手段と、

前記検出手段により前記ＩＣカードの装着が検出された後に任意のモード指定を受け付ける受付手段と、

前記受付手段において前記ＩＣカードの挿入が検出されてから一定時間が経過しても任意のモード指定を受け付けなかった場合に前記センタ口座から現金支払いのための支払いモードに移行するモード移行手段と、

を備えたことを特徴とするＩＣカード取引装置。

【請求項９】　第１財布と第２財布とを有するＩＣカードを使用して支払い取引を行う取引装置であって、

前記取引装置は、

前記第１財布を指定して支払い要求額を入力した際に、暗号化および暗証による支払い承認処理後、前記第１財布に格納された金額が取引要求金額に満たない場合、前記第２財布に格納された金額を補填して取引を遂行することを特徴とする取引装置。

【請求項１０】　第１財布と第２財布とを備え、前記第１財布と第２財布とによる二重財布を用いて取引装置と取引きを行うＩＣカード取引システムに適用されるＩＣカードであって、

前記取引装置から暗証番号とを受信した場合には、前記受信された暗証番号により個人認証処理を行った後、前記取引装置に対して前記第１財布と第２財布に格納される各金額を出力し、一方、前記取引装置から暗証番号を受信しなかった場合には、前記取引装置に対して前記第２財布の金額を出力することを特徴とする二重財布を有したＩＣカード取引システムに適用されるＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ＩＣカードを利用して電子現金を取り扱う電子財布システムおよ

びそのＩＣカード、二重財布を有するＩＣカード取引装置、ならびに、二重財布を有するＩＣカード取引システムおよびそのＩＣカードに関する。

【０００２】

【従来の技術】

近年、ＩＣカードに書き換え可能な不揮発性メモリとマイクロコンピュータ（マイコン）を内蔵させたＩＣカードが普及し、一方、金融機関の間でこのＩＣカードに銀行口座の預金額をこのＩＣカードを転送させてＩＣカード担体で銀行取引や商店での商品購入ができるいわゆる電子財布システムが各種提唱されている。

【０００３】

従来の電子財布システムでは、一般にＩＣカードには、財布は一つ設けられ、その財布へ端末を通じて希望の金額を引き下ろしたり、あるいは、その財布から端末を通じて支払いをするという形態になっている。そして、ＩＣカードの電子財布には、安全性を高めるために高度のセキュリティ機能が一般的には付与され、このために実際の取引処理をする際に操作の遅延や、処理の遅延があった。

【０００４】

特に、従来の電子財布システムの場合、ＩＣカード内の１つのメモリ領域を外部の装置がアクセスする場合、カード所有者の暗証番号をカード内で照合して認証し、また、装置の識別コードを入力して、そのメモリ領域に対してアクセスが許容されている装置であるかどうか照合してはじめて該当領域へのアクセスが許容されるという所謂、照合処理を行うという仕組みになっている。

【０００５】

また、セキュリティを上げるために、ＩＣカードと端末との間のデータ転送の際は、データを暗号化して転送しているが、これらの暗号化手法として公開キーや秘密キーをそれぞれの装置とＩＣカードとが持ち、場合によってはキーを取引処理の都度、両者の間で交換した後、データを暗号化するという、所謂認証処理が採用されている。この暗号化手法としては、ＲＳＡ方式、ＤＥＳ方式等、装置とＩＣカードに共通の鍵データを持ったり、公開鍵、秘密鍵をそれぞれが持ち、共通のアルゴリズムで送信データを暗号化し、復号化するという手法があり、一

般に採用されている。一方、ＩＣカードの利用は各所で考えられている。一般商店やスーパーマーケット等におけるＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅ）システム、病院等におけるカルテシステム、パチンコ等の遊技場における遊技システム、競馬等の投票券システム、公衆電話機や交通等の切符システム等、多岐に亘っている。

【０００６】

この種の近似技術として、例えば特開平２－２０５９３３号公報がある。この公報によれば、自動販売機や店舗における商品購入時の支払いをキャッシュレスで行うためにＩＣカードを用いたシステムが開示されている。具体的には、システムに使用されるＩＣカードのメモリに、プリペイドエリアとオフライン口座エリアとが設けられている。一方のプリペイドエリアは、残高を記憶しておき、ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を用いてその残高で現金取引を行うために使用されるエリアである。他方のオフライン口座エリアは、オフライン口座としての残高を記憶しておき、プリペイドエリアの残高を増額するために個人認証番号を用いてその残高をプリペイドエリアに移動させるために使用されるエリアである。

【０００７】

【発明が解決しようとする課題】

上記公報のように従来例によるＩＣカードシステムでは、電子財布システムに連携させたシステムが各種提案されているが、いずれもＩＣカードに設けられた一つの電子財布からＰＩＮなどを用いての一定の認証処理や一定の照合処理を経由して、暗証照合が成立した場合にのみメモリへのアクセスが可能となった。しかるに、これらのシステムでは、ＩＣカードの不正な捨得の際の安全対策が上述した暗号化技術によって強化されているため、電子財布システムと他のシステムとを連携するには、以下に述べる問題があった。

【０００８】

まず、それぞれの利用装置にそれらの認証処理や照合処理のための入力機能を設ける必要があり、セキュリティ上、利用装置側の構成が複雑化していた。

【０００９】

また、各システムの利用装置を取り扱う人等、利用装置の所有者或いは、そのソフトウェアの関係者にくまなくシステム全体で使用している共通の暗号化のためのアルゴリズムやキー等が判明してしていた。これにより、各所有者による不正がシステム全体のアクセスを可能にすることから、セキュリティを保持することが不可能であった。それゆえ、システム全体では大きな金額の不正の可能性があり、安全性の面で広い地域や１枚のカードの多面的な利用、所謂マルチユースで利用することが難しかった。

【００１０】

また、利用者側からみると、前述した公報（特開平２－２０５９９３号公報）のように取引き時にＰＩＮを入力する等、すべての利用に際して暗証番号の入力が必要となるため、操作が煩雑であった。また、システム上、上述した照合処理が存在するため、実際に取引きが終了するまでに処理はかなりの時間を要していた。このように、取引時間が必要以上にかかりすぎると、例えば、スーパーマーケットでの混雑時の利用、投票券システムにおける出走直前での券購入時の利用、切符システムにおける出発間際の切符購入等の利用等、緊急時の取引処理での利用が阻害されることになった。

【００１１】

また、遊技場等における利用の際は、内心は当日の使用金額をあらかじめ決めていたとしても、いつの間にか財布に入っている全額を使い切ってしまうという問題が指摘されているが、現状では、電子財布に入っている金額はすべて使用できることから、電子財布の利用金額を制限することは不可能であった。

【００１２】

この発明は、ＩＣカードの二重財布としての特性を生かし、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能な二重財布を有する電子財布システムを提供することを第１の目的とする。

【００１３】

この発明は、第１目的を提供する電子財布システムに適用される二重財布すな

わちＩＣカードを提供することを第２の目的とする。

【００１４】

この発明は、二重財布であるＩＣカード上でのセキュリティを一層向上させることが可能な二重財布を有するＩＣカード取引装置を提供することを第３の目的とする。

【００１５】

この発明は、二重財布（ＩＣカード）としての特性を生かし、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させるカード取引を実現することが可能な二重財布を有するＩＣカード取引システムを提供することを第４の目的とする。

【００１６】

この発明は、第４の目的を提供するＩＣカード取引システムに適用される二重財布すなわちＩＣカードを提供することを第５の目的とする。

【００１７】

【課題を解決するための手段】

上述した課題を解決し、各目的を達成するため、まず、請求項１の発明に係る二重財布を有する電子財布システムは、第１預金額が格納される第１領域と第２預金額が格納される第２領域とを備えた書き換え可能な第１不揮発性メモリと、当該メモリに接続された処理装置と、当該処理装置の動作プログラムを格納した第２不揮発性メモリと、当該処理装置を介して前記第１，第２不揮発性メモリにそれぞれ格納された情報にアクセスするための入力端子を備えた携帯型のカード状担体であって、前記第１不揮発性メモリの第１領域に対応して少なくともカード所有者の個人認証番号が前記第１不揮発性メモリに格納され、前記第１不揮発性メモリの第２領域に対応して当該第２領域へのアクセスを許容できる装置の種類を示す識別情報が前記第１不揮発性メモリに格納され、前記第１領域へのアクセスに際して前記入出力端子から入力され暗号化された情報を解読し、その解読された情報に含まれる暗証番号と前記第１不揮発性メモリに格納された個人認証番号とが所定の関係である場合にアクセスを許容し、前記第２領域へのアクセス

に際してアクセスする取引装置の種類を示す識別番号が一致する場合、前記第２領域へのアクセスを許容するカード状担体と、預金額が格納された口座ファイルを有するセンタシステムと、前記カード状担体のメモリの第１領域に、前記センタシステムの預金額の一部または全部を移送するための前記センタシステムに直接または間接的に連携された引出装置であって、装置の識別情報と、カード所有者が入力した暗証番号の内、少なくとも一方を暗号化して前記カード状担体に転送する引出装置と、暗証番号および前記カード状担体における前記第１領域から前記第２領域に転送すべき金額を入力する入力手段と、前記カード状担体に対して前記入力手段によって入力された暗証番号と転送金額と識別情報とを供給する転送装置と、前記カード状担体の第２領域に格納された預金額を使用するため、利用金額と装置情報とを送出する利用装置と、を備え、前記カード状担体は、前記転送装置によって転送を指示され、かつ前記個人認証番号が許容された場合には、前記第１領域に格納された預金額を指定された金額分減算して前記第１領域の更新を行うとともに、前記第２領域に前記指定された金額を書き込み、前記利用装置により利用金額を指示され、かつ前記識別情報が前記第２領域へのアクセスを許容された場合には、前記利用金額を減算して前記利用装置での前記利用金額の利用を許容することを特徴とする。

【００１８】

この請求項１の発明によれば、転送装置を用いた取引きの場合、暗証番号を用いた個人認証を通じてカード状担体の第１領域（第１財布）から第２領域（第２財布）への預金額の転送を行い、利用装置を用いた取引きの場合、個人認証を必要とせずに、カード状担体の第２領域で利用金額を利用するようにしたので、二重財布（ＩＣカード）としての特性が生かされ、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能である。

【００１９】

また、請求項１の発明は、請求項２のように、カード状担体の第２不揮発性メモリに第２領域が引出処理のみ許容するプログラムを格納するようにしてもよい

【００２０】

また、請求項１の発明は、請求項３の発明のように、カード状担体に設けた第３領域に当該第３領域へのアクセスを許容する利用装置の識別情報および暗証番号を登録しておき、利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に第３領域の加算又は減算を許容するようにしてもよい。

【００２１】

また、請求項３の発明は、請求項４の発明のように、カード状担体の第３領域に、加算処理した利用装置を示す識別情報と加算処理した額とを履歴情報として格納するようにしてもよい。

【００２２】

また、請求項５の発明に係る二重財布を有する電子財布システムは、請求項２の発明において、前記カード状担体は、前記利用装置が前記第１不揮発性メモリの領域を指定せずに支払い処理を要求した際に、前記利用装置からの転送情報の復号化処理をスキップして、前記第２預金額から指定された金額情報を差し引く取引きを許容することを特徴とする。

【００２３】

この請求項５の発明によれば、利用装置が領域指定せずに支払い処理を要求した場合には、第２領域の預金額を用いて、セキュリティの低い、個人認証を伴わない簡易な利用取引きを実現することが可能である。

【００２４】

また、請求項６の発明に係る二重財布を有する電子財布システムに適用されるＩＣカードは、第１金額が記憶された第１財布、第２金額が記憶された第２財布、支払い処理プログラム、利用者の暗証番号プログラムを格納したメモリと、前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、外部装置と通信を遂行する通信手段と、を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって、前記支払いプログラムは、外部の支払い要求装置から、財布を指定せずに支払いコマンドを受信した場合、前記

第２財布に格納された第２金額に基づき支払い処理し、前記第１財布を指定した支払いコマンドを受信した場合、暗証照合を行い、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする。

【００２５】

この請求項６の発明によれば、外部から財布の指定がなかった場合には第２財布に格納された第２金額に基づき支払いを行い、外部から第１財布が指定された場合には暗証照合を行ってから第１財布での支払いを行うようにしたので、セキュリティの低い第２財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第１財布については個人認証により不正防止を図ることが可能である。

【００２６】

また、請求項７の発明に係る二重財布を有する電子財布システムに適用されるＩＣカードは、第１金額が記憶された第１財布、第２金額が記憶された第２財布、支払い処理プログラムおよび暗号化／復号化プログラムを格納したメモリと、前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、外部装置と通信を遂行する通信手段と、外部の取引装置とのインタフェースを司るインタフェース手段と、を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって、前記支払いプログラムは、前記インタフェース手段を通じて外部装置から第１財布を指定せずにコマンドを受信した場合、前記第２財布に格納された第２金額に基づいて支払い処理を遂行し、前記第１財布を指定した支払いコマンドを受信した場合、前記暗号化および復号化プログラムを使用して、外部の装置と通信し、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする。

【００２７】

この請求項７の発明によれば、外部から財布の指定がなかった場合には第２財布に格納された第２金額に基づき支払いを行い、外部から第１財布が指定された場合には暗号化および復号化を通じて第１財布での支払いを行うようにしたので、セキュリティの低い第２財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第１財布については暗号利用により不

正防止機能を一層向上させることが可能である。

【００２８】

また、請求項８の発明に係るＩＣカード取引装置は、ＩＣカードに格納される金額とセンタ口座に格納される金額との内の一方を選択し、その選択された金額に基づいて現金支払いを行うＩＣカード取引装置であって、ＩＣカードの装着を検出する検出手段と、前記検出手段により前記ＩＣカードの装着が検出された後に任意のモード指定を受け付ける受付手段と、前記受付手段において前記ＩＣカードの挿入が検出されてから一定時間が経過しても任意のモード指定を受け付けなかった場合に前記センタ口座から現金支払いのための支払いモードに移行するモード移行手段と、を備えたことを特徴とする。

【００２９】

この請求項８の発明によれば、取引装置とＩＣカードとの取引きで、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引きについてはモードによるバリエーションを持たせ、現金での取引きについてはその指定操作を省くことで、現金取引きの簡略化を実現することが可能である。

【００３０】

また、請求項９の発明に係る取引装置は、第１財布と第２財布とを有するＩＣカードを使用して支払い取引を行う取引装置であって、前記取引装置は、前記第１財布を指定して支払い要求額を入力した際に、暗号化および暗証による支払い承認処理後、前記第１財布に格納された金額が取引要求金額に満たない場合、前記第２財布に格納された金額を補填して取引を遂行することを特徴とする。

【００３１】

この請求項９の発明によれば、取引装置とＩＣカードとの個人認証を要する取引きで、第１財布だけで金額上の取引きが成立しなくても第２財布の金額を補填して再度取引きを遂行するようにしたので、利用者が取引きのための金額を気にすることなく取引きを遂行することができ、操作性の向上を図ることが可能である。

【００３２】

この請求項１０の発明に係るＩＣカード取引システムに適用されるＩＣカードは、第１財布と第２財布とを備え、前記第１財布と第２財布とによる二重財布を用いて取引装置と取引きを行うＩＣカード取引システムに適用されるＩＣカードであって、前記取引装置から暗証番号とを受信した場合には、前記受信された暗証番号により個人認証処理を行った後、前記取引装置に対して前記第１財布と第２財布に格納される各金額を出力し、一方、前記取引装置から暗証番号を受信しなかった場合には、前記取引装置に対して前記第２財布の金額を出力することを特徴とする。

【００３３】

この請求項１０の発明によれば、取引装置とＩＣカードとの取引きで、個人認証を経た場合にのみ第１財布および第２財布の金額を取引装置に出力し、そうでない場合には第２財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に教える程度の取引きであっても、個人認証を通過できなければセキュリティの高い第１財布を開くことを防止することが可能である。

【００３４】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係る二重財布を有する電子財布システム、その電子財布システムに適用されるＩＣカード、二重財布を有するＩＣカード取引装置、二重財布を有するＩＣカード取引システムおよびそのＩＣカード取引システムに適用されるＩＣカードの好適な実施の形態を詳細に説明する。

【００３５】

まず、システム構成について説明する。図１はこの発明の実施の形態による電子財布システム（ＩＣカード取引システム含む）の一例を示す構成図である。図１に示した電子財布システムは、ＩＣカード１，ＩＣカード１との取引装置である引出装置２，ＩＣカード１との取引装置である利用装置４，センタシステム３より構成される。

【００３６】

ＩＣカード１は、取引の際に暗証番号（ＰＩＮの意味）および暗号化を必要とするセキュリティの高い第１財布１Ａと取引の際に暗証番号および暗号化を必要

としないセキュリティの低い第２財布１Ｂとからなる二重財布機能を有している。引出装置２は、ＩＣカード１を着脱自在とした構成であり、銀行などのセンタシステム３との通信を通じて引き出した預金をＩＣカード１の第１財布１Ａに格納する。

【００３７】

センタシステム３は、銀行などのように利用者の預金を管理しており、引出装置２などの機器との通信を通じて預金の引き落としなどを行う。利用装置４は、ＩＣカード１を着脱自在とした構成であり、ＩＣカード１の第２財布１Ｂに格納された金額で各種のサービスを提供する。

【００３８】

つぎに、ＩＣカード１について詳述する。まず、原理について説明する。図２は図１に示したＩＣカード１を機能的に示すブロック図である。図２に示したＩＣカード１は、機能として、要求領域識別部１１，復号化セキュリティ処理部１２，暗証番号処理部１３，照合処理部１４，アクセス権確認処理部１５および取引処理部１６を備えている。

【００３９】

要求領域識別部１１は、端末に自ＩＣカード１が装着された際に、第１財布１Ａや第２財布１Ｂの領域を要求しているか、もしくはいずれの領域についても要求していないかを識別する。この要求領域識別部１１は、領域要求がない場合に照合処理部１４に処理を移す。復号化セキュリティ処理部１２は、要求領域識別部１１で領域を要求している場合に端末から暗号化されて受信される情報を、復号化キーを使用して復号化する。

【００４０】

復号化暗証番号処理部１３は、暗証番号による個人認証処理を行う。照合処理部１４は、自ＩＣカード１を装着した端末がアクセスしてよい端末か否かを照合する。アクセス権確認処理部１５は、照合結果からアクセス権の有無を確認する。取引処理部１６は、アクセス権有りの確認後に相手端末との間で取引きを行う。

【００４１】

続いて上述したＩＣカード１の原理を実現するハードウェア構成について説明する。図３は図１に示したＩＣカード１をハードウェア的に示すブロック図である。図３に示したＩＣカード１は、相手端末と接続するための端子１０１，相手端末と自ＩＣカード１内部とのインタフェースを司るインタフェース（Ｉ／Ｆ）１０２，ＣＰＵ１０３，ＲＯＭ１０４，ＲＡＭ１０５，ＥＥＰＲＯＭ１０６等により構成される。

【００４２】

ＣＰＵ１０３は、ＲＯＭ１０４に格納されたプログラムに従って全体の処理を制御する。ＲＯＭ１０４は、後述する図８～図１７のフローチャートに従うプログラムを格納している。ＲＡＭ１０５は、ＣＰＵ１０３のワークエリアとして使用される。

【００４３】

ＥＥＰＲＯＭ１０６は、不揮発性メモリであり、前述した第１財布１Ａ，第２財布１Ｂそれぞれの機能を実現するために使用される第１財布エリア１０６Ａ，第２財布エリア１０６Ｂと、相手端末との取引履歴を記録するために使用される第３財布エリア１０６Ｃとを有している。

【００４４】

つぎに、上述したＩＣカード１の二重財布構造について説明する。図４は図３に示したＩＣカード１のメモリ構成例を示す図である。ＩＣカード１の二重財布構造は、第１財布エリア１０６Ａと第２財布エリア１０６Ｂとで形成される。具体的には、ＩＣカード１のＥＥＰＲＯＭ１０６は、図４（ａ）に示したディレクトリ領域と図４（ｂ）に示したデータ領域とに区分される。

【００４５】

ディレクトリ領域は、図４（ａ）に示したように、第１財布エリア１０６Ａの第１ディレクトリＤ１、第２財布エリア１０６Ｂの第２ディレクトリＤ２、第３財布エリア１０６Ｃの第３ディレクトリＤ３とにより構成される。

【００４６】

第１ディレクトリＤ１は、第１財布エリア１０６Ａのアドレス（第１財布アドレス）、要求時のセキュリティのためのＰＩＮである暗証番号、および相手端末

の機械ＩＤとそのアクセス権との対により構成される。図４（ａ）の例では、第１財布アドレスは“Ｆ００１～Ｆ００Ｆ”、暗証番号は“１２３４”、機械ＩＤおよびアクセス権は相手端末＃１，＃２にそれぞれ対応して任意に設定される。アクセス権としては、書き込み、読み出し、更新、消去などがある。

【００４７】

第２ディレクトリＤ２は、第２財布エリア１０６Ｂのアドレス（第２財布アドレス）、その設定をフリーとする暗証番号、および相手端末の機械ＩＤとそのアクセス権との対により構成される。図４（ａ）の例では、第２財布アドレスは“Ｆ０１１～Ｆ０１Ｆ”、暗証番号はフリー、機械ＩＤおよびアクセス権は相手端末に対応して任意に設定される。

【００４８】

第３ディレクトリＤ３は、第３財布エリア１０６Ｃのアドレス（第３財布アドレス）、要求時のセキュリティのためのＰＩＮである暗証番号、および相手端末の機械ＩＤとそのアクセス権との対により構成される。図４（ａ）の例では、第３財布アドレスは“Ｆ０２１～Ｆ０３Ｆ”、暗証番号は“１２３４”、機械ＩＤおよびアクセス権は相手端末＃１，＃２にそれぞれ対応して任意に設定される。

【００４９】

そして、図４（ｂ）に示したデータ領域は、第１財布エリア１０６Ａ，第２財布エリア１０６Ｂ，第３財布エリア１０６Ｃ，追加情報としてのセンタ口座情報に区分される。

【００５０】

第１財布エリア１０６Ａに関して、第１ディレクトリＤ１の第１財布アドレスにより領域が特定され、第１財布としての残金が格納される。第２財布エリア１０６Ｂに関して、第２ディレクトリＤ２の第２財布アドレスにより領域が特定され、第２財布としての残金が格納される。第３財布エリア１０６Ｃに関して、第３ディレクトリＤ３の第３財布アドレスにより領域が特定され、第３財布として第１財布と第２財布の合計額，取引履歴（取引日，取引機械ＩＤ，取引金額等）等が格納される。なお、センタ口座情報には、センタシステム３における口座番号などの情報が含まれている。

【００５１】

つぎに、図１に示した引出装置２について詳述する。図５は図１に示した引出装置２を機能的に示すブロック図である。図５に示した引出装置２は、装置識別ＩＤレジスタ２１，認証転送処理部２２，暗号化処理部２３，入力部２４により構成される。

【００５２】

機械ＩＤレジスタ２１は、ＩＣカード１が機械を識別できるように機械毎に割り当てられた機械ＩＤを格納している。認証転送処理部２２は、センタシステム３から預金を引き出す際に暗証番号および引出金額から認証を行って引出金額を暗号化処理部２３に転送する。暗号化処理部２３は、機械ＩＤレジスタ２１に格納された機械ＩＤや入力部２４で入力された暗証番号を暗号化してＩＣカード１に送信する。入力部２４は、利用者の手操作により暗証番号や引出金額を入力してこれら入力情報を認証転送処理部２２に送出する。

【００５３】

つぎに、図１に示したセンタシステム３について詳述する。図６は図１に示したセンタシステム３を概略的に示す構成図である。図６に示したセンタシステム３は、引出装置２などに回線で接続されたホストコンピュータ３１，各預金者の口座情報を記録したデータベース３２などにより構成される。

【００５４】

ホストコンピュータ３１は、データベース３２をアクセスして、引出装置２などから預金の引き落とし等の処理を行う。データベース３２は、ホストコンピュータ３１からアクセスされ、ホストコンピュータ３１の要求に応じて所要の口座から預金の一部もしくは全部を引出すなどの処理を行う。

【００５５】

つぎに、図１に示した利用装置４について詳述する。図７は図１に示した利用装置４を機能的に示すブロック図である。図７に示した利用装置４は、機械ＩＤレジスタ４１，転送処理部４２，支払額発生部４３，取引処理部４４，受信部４５，メモリ４６により構成される。

【００５６】

機械ＩＤレジスタ４１は、ＩＣカード１が機械を識別できるように機械毎に割り当てられた機械ＩＤを格納している。転送処理部４２は、特に引出装置２のような認証を必要とせず、サービスを受けるのに必要な支払い額を支払額発生部４３から受け取ってＩＣカード１に転送する。また、転送に当たっては暗号化処理は行わない。支払額発生部４３は、サービスを提供するのに必要な支払い額を発生して、その支払い額を転送処理部４２と取引処理部４４とに送出する。

【００５７】

取引処理部４４は、ＩＣカード１からの要求に応じてサービス提供のための支払い額に応じた取引処理を実行する。受信部４５は、ＩＣカード１の装着によりサービスに必要な支払い額を受け取り、その通知を取引処理部４４に送出するとともに、サービスの履歴情報をメモリ４６に送出する。メモリ４６は、受信部４５からＩＣカード１の履歴情報を受け取って記憶する。

【００５８】

つぎに、上述した電子財布システムの動作について説明する。まず、ＩＣカード１の動作について説明する。図８および図９は実施の形態によるＩＣカード１のメイン動作を説明するフローチャートである。なお、すでにＩＣカード１は、相手端末（引出装置２もしくは利用装置４）に装着されているものとする。

【００５９】

具体的には、ＩＣカード１は、まず、相手端末との間で前処理を実行する（ステップＳ１０１）。この前処理は、ＩＣカード１を利用できる端末かどうかを相手端末との交信により確認するものであり、その詳細は後述（図１６および図１７）する。続いて、相手端末よりコマンド受信が行われ（ステップＳ１０２）、その受信されたコマンドに第１財布エリア１０６Ａもしくは第２財布エリア１０６Ｂを要求する領域ＩＤが含まれているか否か判断される（ステップＳ１０３）。なお、この受信コマンドには、機械ＩＤとアクセス権との対などが含まれているが、領域ＩＤについては任意に設定される。

【００６０】

ステップＳ１０３において、もし領域ＩＤが含まれていると判断された場合には、処理はステップＳ１０４に移行し、一方、含まれていないと判断された場合

には、処理はステップＳ１１２（図９参照）に移行する。

【００６１】

まず、処理がステップＳ１０４に移行した場合には、受信コマンドに含まれている領域ＩＤから第１財布エリア１０６Ａと第２財布エリア１０６Ｂとのいずれの領域が要求されているかを読み取る処理が実行される。さらに受信コマンドに含まれている機械ＩＤとＩＣカード１のＥＥＰＲＯＭ１０６に格納されている機械ＩＤとの比較が行われ、両機械ＩＤが一致していれば、処理はステップＳ１０６に移行し、一方、一致していなければ、このＩＣカード１は相手端末を利用できないものとして処理は無効とされる（ステップＳ１０５）。

【００６２】

ステップＳ１０６では、ＥＥＰＲＯＭ１０６に機械ＩＤと対で記憶されているアクセス権と受信コマンドに含まれるアクセス権（受信アクセス）との対応が確認される。その結果、両アクセス権が対応していると判断された場合には、処理はステップＳ１０７に移行するが、対応していないと判断された場合には、このＩＣカード１は相手端末をアクセスできないものとして処理は無効とされる。

【００６３】

ステップＳ１０７では、ステップＳ１０４で読み取られた領域が第１財布エリア１０６Ａであった場合には、続くステップＳ１０８において相手端末からの要求内容が判別され、一方、第２財布エリア１０６Ｂであった場合には、他モードとして処理が実行される。

【００６４】

ステップＳ１０８において、要求内容が転送であれば、処理はステップＳ１０９に移行して転送処理（図１０、図１１参照）を実行し、支払いであれば、処理はステップＳ１１０に移行して支払い処理（図１２および図１３参照）を実行し、カード預金であれば、処理はステップＳ１１１に移行してカード預金処理（図１５および図１６参照）を実行する。以上の転送処理，支払い処理，カード預金処理のいずれかが終了した後に、本処理は終了する。

【００６５】

また、ステップＳ１０３で受信コマンドに領域ＩＤが含まれていなかった場合

には、強制的に支払いモードとしての処理が開始される。まず、ステップＳ１１２（図９参照）において、強制的にＥＥＰＲＯＭ１０６の第２ディレクトリＤ２にある第２財布アドレスが読み出される。そして、同第２ディレクトリＤ２に格納される機械ＩＤが受信コマンド中の機械ＩＤと比較され、一致していれば、処理はステップＳ１１４に移行するが、一致していなければ、このＩＣカード１は相手端末を利用できないものとして処理は無効とされる。

【００６６】

ステップＳ１１４では、ステップＳ１１２で読み出した第２財布アドレスから第２財布エリア１０６Ｂに格納されているデータすなわち残高が読み込まれる。続いてその読み込まれた第２財布エリア１０６Ｂの残高は相手端末に出力される（ステップＳ１１５）。この残高の出力により相手端末側では、第２財布に入っている金額を知ることが出来る。そして、ＩＣカード１に対して要求額（支払い額）を含んだ支払いコマンドが出力される。

【００６７】

続いて、相手端末から一定時間内に支払いコマンドが受信されると（ステップＳ１１６）、続くステップＳ１１７において第２財布エリア１０６Ｂに格納されている残高から相手端末が支払いを要求する金額すなわち要求額が差し引かれる。その結果得られた金額はＲＡＭ１０５にあらかじめ設けられたワークエリアＷ１に格納される。なお、ステップＳ１１６において支払いコマンドの受信がなかった場合には、相手端末との支払い取引きはなかったものとして処理は終了する。

【００６８】

そして、このワークエリアＷ１に格納された金額がゼロもしくはプラスであれば（ステップＳ１１８）、第２財布だけで相手端末が要求する支払いが可能であることから、相手端末に対して、支払い可としてその支払い可の情報と支払い額（要求額を意味する）とが通知される（ステップＳ１１９）。なお、ステップＳ１１８においてワークエリアＷ１の金額がマイナスを示していた場合には、相手端末との支払い取引きはなかったものとして処理は終了する。

【００６９】

ステップＳ１１９において通知が行われた後、一定時間が経過しても相手端末からその通知に対する応答が行われなかった場合には（ステップＳ１２０）、ワークエリアＷ１に格納された金額はクリアされ、相手端末との支払い取引きはなかったものとして処理は終了する。一方、一定時間内に相手端末から応答受信が入った場合には（ステップＳ１２０）、その応答受信から受け取りコードが受信される（ステップＳ１２１）。

【００７０】

このように、相手端末から受け取りコードが受信されると、その相手端末において支払いに応じた処理が実行されたことになるため、第２財布エリア１０６Ｂの残高が更新される。すなわち、ワークエリアＷ１の金額が第２財布エリア１０６Ｂに格納され（ステップＳ１２２）、併せてその支払い取引きの日付が第３財布エリア１０６Ｃに履歴として格納される（ステップＳ１２３）。最後に、相手端末に対してＩＣカード１内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップＳ１２４）。

【００７１】

つぎに、上述したメイン動作の個々の動作について説明する。まず、転送処理（図８のステップＳ１０９）について説明する。図１０および図１１は図８に示したメイン動作における転送処理を説明するフローチャートである。この転送処理は、ＩＣカード１が引出装置２に装着された場合を想定しており、引出装置２を用いて残金が不足している第２財布に対して第１財布に入っている残金の一部（転送要求額）を転送するものである。この転送処理には、第１財布のセキュリティ上、ＰＩＮである暗証番号および暗号化／復号化の処理が必要となる。

【００７２】

この転送処理では、まず、相手端末からの転送要求額が受信され、その転送要求額が復号される（ステップＳ１００１）。続いて、第１財布エリア１０６Ａに格納された残高から復号された転送要求額が差し引かれ、その金額がＲＡＭ１０５にあらかじめ設けておいたワークエリアＷ２に格納される（ステップＳ１００２）。このワークエリアＷ２に格納された金額は、第１財布から第２財布に転送要求額を転送したと仮定した場合の第１財布の残高を示している。

【００７３】

ここでは、第１財布へのアクセスとなり、転送取引きそのものが高度なセキュリティを伴うことから、暗証番号による個人認証が必要となる。そのため、相手端末に対して暗証番号が要求される（ステップＳ１００３）。この後、相手端末から暗証番号が送信されるまで一定時間受信待ちとなる（ステップＳ１００４）。なお、一定時間を経過しても暗証番号が受信されない場合には、図示せぬがこの転送取引きは終了する。

【００７４】

そして、相手端末から暗証番号が受信され（ステップＳ１００４）、ステップＳ１００２でワークエリアＷ２に格納された金額がゼロもしくはプラスであった場合には（ステップＳ１００５）、ステップＳ１００４で受信された暗証番号が復号される（ステップＳ１００６）。一方、ワークエリアＷ２に格納された金額がマイナスであった場合には（ステップＳ１００５）、この転送取引きはなかったものとして無効にされる。

【００７５】

ステップＳ１００６で暗証番号が復号されると、続くステップＳ１００７において、第１ディレクトリＤ１に格納されている暗証番号が読み出され、その暗証番号が復号される。そして、この復号されたＩＣカード１自身の暗証番号と相手端末から受け取って復号した暗証番号との照合が行われ（ステップＳ１００８）、両暗証番号が一致した場合には（ステップＳ１００９）、認証および照合をパスできたものとして処理はステップＳ１０１０に移行する。一方、認証および照合をパスできなかった場合には、この転送取引きはなかったものとして無効にされる。

【００７６】

ステップＳ１０１０では、第２財布エリア１０６Ｂに格納されている金額（残高）に転送額（前述の転送要求額）が加算され、その合計がワークエリアＷ１に格納される。このワークエリアＷ１に格納された金額は、第１財布から第２財布に転送額を転送したと仮定した場合の第２財布の残高を示している。

【００７７】

続いて、この転送取引きでは認証および照合のパスに応じて転送可となることから、ワークエリアＷ１，Ｗ２に格納された金額がそれぞれ暗号化される（ステップＳ１０１１）。このようにして暗号化された各金額は暗号化情報として相手端末に送信される（ステップＳ１０１２）。

【００７８】

その後、相手端末から一定時間内に応答受信がない場合には（ステップＳ１０１３）、処理はステップＳ１０１４に移行して、この転送取引きはなかったものにするため、ワークエリアＷ１，Ｗ２はいずれもクリアされる。その後、処理はメイン処理（図８参照）に戻る。一方、ステップＳ１０１３において応答受信が確認された場合には、その応答受信によって受信されたデータが了解コードか否か判断される（ステップＳ１０１５）。この了解コードは、相手端末において利用者が要求する転送の了解を意味するものである。

【００７９】

ステップＳ１０１５において受信データが了解コードであった場合には、転送取引きが成立したものとして、まずワークエリアＷ２の暗号化された金額が第１財布エリア１０６Ａに格納され（ステップＳ１０１７）、さらにワークエリアエリアＷ１の暗号化された金額が第２財布エリア１０６Ｂに格納される（ステップＳ１０１８）。このようにして、第１財布エリア１０６Ａと第２財布エリア１０６Ｂとは、転送要求金額に従って残高が更新される。なお、ステップＳ１０１５において受信データが了解コードでなかった場合には、転送取引きが成立しないものとして、続くステップＳ１０１６において相手端末にコメンド再送要求が行われ、処理はメインのステップＳ１０２（図８参照）に戻る。

【００８０】

さらに、第３財布エリア１０６Ｃには、上述した転送取引きの日付などの情報が履歴として格納される（ステップＳ１０１９）。最後に、相手端末に対してＩＣカード１内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップＳ１０２０）。

【００８１】

続いて、支払い動作（図８のステップＳ１１０）について説明する。図１２お

よび図１３は図８に示したメイン動作における支払い処理を説明するフローチャートであり、図１４は図１２に示した支払い処理における追加取引を説明するフローチャートである。この支払い処理は、ＩＣカード１が引出装置２に装着された場合を想定しており、引出装置２を用いて第１財布に入っている残金の一部（転送要求額）を引出装置２に支払うものである。この支払い処理には、第１財布のセキュリティ上、ＰＩＮである暗証番号が必要となる。

【００８２】

この支払い処理では、まず、相手端末に対して暗証番号および要求額が要請される（ステップＳ１１０１）。その後、暗証番号および要求額が受信されると（ステップＳ１１０２）、まず要求額が復号される（ステップＳ１００３）。続いて、第１財布エリア１０６Ａに格納された残高から復号された要求額が差し引かされ、その金額がＲＡＭ１０５のワークエリアＷ２に格納される（ステップＳ１００４）。このワークエリアＷ２に格納された金額は、第１財布から引出装置２に要求額を支払ったと仮定した場合の第１財布の残高を示している。

【００８３】

そして、ステップＳ１１０４でワークエリアＷ２に格納された金額がゼロもしくはプラスであった場合には（ステップＳ１１０５）、今度はステップＳ１１０２で受信された暗証番号が復号される（ステップＳ１１０７）。一方、ワークエリアＷ２に格納された金額がマイナスであった場合には（ステップＳ１１０５）、処理はステップＳ１１０６に移行して追加取引（図１４参照）を実行する。

【００８４】

ステップＳ１１０７で暗証番号が復号されると、続くステップＳ１１０８において、第１ディレクトリＤ１に格納されている暗証番号が読み出され、その暗証番号が復号される。そして、この復号されたＩＣカード１自身の暗証番号と相手端末から受け取って復号した暗証番号との照合が行われ（ステップＳ１１０９）、両暗証番号が一致した場合には（ステップＳ１１１０）、認証をパスできたものとして処理はステップＳ１１１１に移行する。一方、認証をパスできなかった場合には、この支払い取引きはなかったものとして無効にされる。

【００８５】

ステップＳ１１１１では、この支払い取引きでは認証のパスに応じて支払い可となることから、ワークエリアＷ２に格納された金額が暗号化される。このようにして暗号化された金額は暗号化情報として相手端末に送信される（ステップＳ１１１２）。

【００８６】

その後、相手端末から一定時間内に応答受信がない場合には（ステップＳ１１１３）、処理はステップＳ１１１５に移行して、この支払い取引きはなかったものにするため、ワークエリアＷ２はクリアされる。その後、処理はメイン処理（図８参照）に戻る。一方、ステップＳ１１１３において応答受信が確認された場合には、その応答受信によって受信されたデータが受け取りコードか否か判断される（ステップＳ１１１４）。この受け取りコードは、相手端末において利用者が要求する支払いの受け取り完了を意味するものである。

【００８７】

ステップＳ１１１４において受信データが受け取りコードであった場合には、支払い取引きが成立したものとして、ワークエリアＷ２の暗号化された金額が第１財布エリア１０６Ａに格納される（ステップＳ１１１６）。このようにして、第１財布エリア１０６Ａは、支払い要求金額に従って残高が更新される。

【００８８】

さらに、第３財布エリア１０６Ｃには、上述した転送取引きの日付などの情報が履歴として格納される（ステップＳ１１１７）。最後に、相手端末に対してＩＣカード１内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップＳ１１１８）。

【００８９】

さて、上述したステップＳ１１０６による追加取引（図１４参照）はつぎのように処理される。すなわち、まず、ステップＳ１５０１において第２財布エリア１０６Ｂの残高が読み出され、続くステップＳ１５０２においてその読み出された残高がすでにステップＳ１１０４でワークエリアＷ２に格納された金額に加算される。すなわち、この合計によりワークエリアＷ２の格納額が更新される。

【００９０】

そして、ステップＳ１１５０２で更新されたワークエリアＷ２の格納額がゼロもしくはプラスであった場合には（ステップＳ１５０３）、処理はステップＳ１５０４に移行するが、ワークエリアＷ２の格納額がマイナスであった場合には（ステップＳ１５０３）、第１財布の残高に第２財布の残高を加算しても支払要求額を満たせないことから、この支払い取引きはなかったものとして無効にされる。

【００９１】

処理がステップＳ１５０４に移行すると、第１財布の残高に第２財布の残高を加算した額が支払要求額を満たすことから、支払い可としての処理が続行される。そのために、処理は前述したステップＳ１１０７に戻り、同様の処理を実行する。ただし、この追加取引を含むことで第２財布エリア１０６Ｂの残高が使用されたことから、ステップＳ１１１６では、この追加取引を含む場合にのみ第２財布エリア１０６Ｂの格納額がゼロにクリアされる。

【００９２】

さらに続いてカード預金処理（図８のステップＳ１１１）について説明する。図１５および図１６は図８に示したメイン動作におけるカード預金処理を説明するフローチャートである。このカード預金処理は、引出装置２を利用してセンタシステム３から預金を要求額分だけ引出し、その引き出した要求額をＩＣカード１に格納する処理である。このカード預金処理には、第１財布のセキュリティ上、ＰＩＮである暗証番号が必要となる。

【００９３】

まず、相手端末に対して預金要求額を要求し、その相手端末から送られてくる預金要求額を復号する処理が実行される（ステップＳ１２０１）。この預金要求額は相手端末において預金者が入力する情報である。続いてＥＥＰＲＯＭ１０６のデータ領域からセンタ口座情報が読み出され、そのセンタ口座情報に含まれる口座番号が抽出される（ステップＳ１２０２）。

【００９４】

続いて、相手端末に対して暗証番号が要求され（ステップＳ１２０３）、その後に、相手端末から暗号化された暗証番号が受信されると、その暗号化された暗

証番号は復号される（ステップＳ１２０４）。そして、第１財布の暗証番号が第１ディレクトリＤ１より読み出され（ステップＳ１２０５）、その暗証番号が復号される（ステップＳ１２０６）。

【００９５】

さらに、相手端末から送られてきた領域ＩＤからセンタ転送用暗号化キーが読み出され（ステップＳ１２０７）、そのセンタ転送用暗号化キーを用いてステップＳ１２０１で復号された預金要求額とステップＳ１２０２で読み出された口座番号とが暗号化される（ステップＳ１２０８）。このようにして暗号化された情報は暗号化情報としてカード預金要求コマンドに付加されてセンタ送信される（ステップＳ１２０９）。

【００９６】

その後、センタシステム３から要求額が送られてくるまで処理は受信待ちとなる（ステップＳ１２１０）。センタシステム３から要求額が送られてくると（ステップＳ１２１１）、第１財布エリア１０６Ａに格納されている残高が読み取られる（ステップＳ１２１２）。この第１財布の残高に受信された要求額が加算され、その合計がワークエリアＷ２に格納され（ステップＳ１２１３）、そのワークエリアＷ２の格納額が第１財布エリア１０６Ａに格納される。これにより、第１財布エリア１０６Ａへのカード預金が完了する。

【００９７】

そして、要求額，第１財布エリア１０６Ａの残高がそれぞれ暗号化され（ステップＳ１２１５）、その暗号化された情報（暗号化情報）が相手端末に出力される（ステップＳ１２１６）。

【００９８】

つぎに、前述の電子財布システムにおいて実施される復号，暗号化，前処理について説明する。まず、復号処理について説明する。図１７は実施の形態における復号処理を説明するフローチャートである。

【００９９】

図１７に示した復号処理は、電子財布システムに適用される引出装置２，利用装置４，ＩＣカード１にすべて付加される機能である。その機能は、図示せぬが

、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）により実現してもよい。このＤＳＰを適用する場合には、そのＤＳＰ内に復号のための復号回路部が設けられる。

【０１００】

動作としては、まず、領域ＩＤから復号キーが読み出され（ステップＳ１３０１）、ＤＳＰの復号回路部へその復号キーが送信される（ステップＳ１３０２）。相手端末からの受信データから復号部が抽出され（ステップＳ１３０３）、その抽出された復号部が復号回路部へ転送される（ステップＳ１３０４）。このようにして復号回路部には、復号キーと復号部とが揃うので、その段階で復号回路部において復号が行われる。そして、復号回路部からの復号データが受信されると、復号処理は完了する（ステップＳ１３０５）。

【０１０１】

続いて暗号化処理について説明する。図１８は実施の形態における暗号化処理を説明するフローチャートである。図１８に示した暗号化処理は、電子財布システムに適用される引出装置２，利用装置４，ＩＣカード１にすべて付加される機能である。その機能は、図示せぬが、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｉｎａｌ　Ｐｒｏｃｅｓｓｏｒ）により実現してもよい。このＤＳＰを適用する場合には、そのＤＳＰ内に復号のための暗号回路部が設けられる。

【０１０２】

動作としては、まず、領域ＩＤから暗号化キーが読み出され（ステップＳ１４０１）、ＤＳＰの暗号回路部へその暗号化キーが送信される（ステップＳ１４０２）。相手端末からの受信データから暗号化すべきデータが抽出され（ステップＳ１４０３）、その抽出されたデータが暗号回路部へ転送される（ステップＳ１４０４）。このようにして暗号回路部には、暗号化キーと暗号化すべきデータとが揃うので、その段階で暗号回路部において暗号化が行われる。そして、暗号回路部からの暗号化データが受信されると、暗号化処理は完了する（ステップＳ１４０５）。

【０１０３】

さらに続いて前処理について説明する。図１９および図２０は実施の形態にお

ける前処理を説明するフローチャートである。以下に説明する図１９および図２０では、端末側とＩＣカード１間の通信処理が示されている。

【０１０４】

端末は、まず、ＩＣカード１の挿入待ちとなり（ステップＴ１）、一定時間毎に挿入状態が確認される（ステップＴ２）。ＩＣカード１が端末の装着部に挿入されると、端末はその挿入からＩＣカード１のセット状態を確認する（ステップＴ２）。その後、端末は、ＩＣカード１に電源を供給し（ステップＴ３）、さらにリセット信号を送信する（ステップＴ４）。

【０１０５】

ＩＣカード１は、端末から電源供給を受けた後に自身の電源をＯＮし（ステップＣ１）、続いて送られてくるリセット信号に従ってＣＰＵ１０３をリセットする（ステップＣ２）。その後、ＩＣカード１は初期化などを経て、まず自ＩＣカード１で使用できる商用カードの種類（例えばＶＩＳＡカード，マスターカードなど）を読み出す（ステップＣ３）。その読み出されたカード種類はＡＴＲ（Ａｎｓｗｅｒ　Ｔｏ　Ｒｅｓｅｔ）信号に付加されて相手端末に返信される（ステップＣ４）。

【０１０６】

端末は、リセット信号を送信した後にカード種類を受け取ると（ステップＴ４）、そのカード種類から自端末で使用できるカードを識別する（ステップＴ５）。なお、使用できるカードがない場合には、この取引きは強制終了される。また、使用できるカードがあれば、端末は、乱数を発生してその乱数をＩＣカード１に送信するとともに（ステップＴ６）、その乱数を自身の暗号化キーを用いて暗号化する（ステップＴ７）。

【０１０７】

ＩＣカード１は、相手端末から送信されてきた乱数を受信すると（ステップＣ５）、自身の暗号化キーを読み出し（ステップＣ６）、その暗号化キーを用いて受信された乱数を暗号化する（ステップＣ７）。ＩＣカード１は、さらに、その暗号化された乱数を相手端末に送信して（ステップＣ８）、相手端末からの応答を待つ。

【０１０８】

端末は、ＩＣカード１から暗号化された乱数を受信すると（ステップＴ８）、自身で暗号化した乱数とＩＣカード１で暗号化された乱数とを比較する（ステップＴ９）。そして、２つの暗号化された乱数が一致した場合には（ステップＴ１０）、端末側の認証でＩＣカード１が適合するものであるという判断が下される。したがって、端末はＩＣカード１に対して適合応答する（ステップＴ１１）。一方、２つの暗号化された乱数が不一致であった場合には（ステップＴ１０）、端末側の認証でＩＣカード１が不適合するものであるから、この取引きはないものとして処理が終了する。

【０１０９】

端末からＩＣカード１に適合応答が行われた場合には、ＩＣカード１は、その適合応答を受け付けて（ステップＣ９）、今度は自ＩＣカード１側で乱数を発生する。ＩＣカード１は、この乱数を相手端末に送信する（ステップＣ１０）。ＩＣカード１は、この乱数発生とともに、自身の暗号化キーを用いて乱数を暗号化する（ステップＣ１１）。

【０１１０】

端末は、ＩＣカード１から送信されてきた乱数を受信すると（ステップＴ１２）、自身の暗号化キーを読み出し（ステップＴ１３）、その暗号化キーを用いて受信された乱数を暗号化してからＩＣカード１に送信する（ステップＴ１４）。そして、端末は、ＩＣカード１からの応答を待つ。

【０１１１】

ＩＣカード１は、相手端末から暗号化された乱数を受信すると（ステップＣ１２）、自身で暗号化した乱数と相手端末で暗号化された乱数とを比較する（ステップＣ１３）。そして、２つの暗号化された乱数が一致した場合には（ステップＣ１４）、ＩＣカード１側の認証で相手端末が適合するものであるという判断が下される。したがって、ＩＣカード１は相手端末に対して適合応答する（ステップＣ１５）。一方、２つの暗号化された乱数が不一致であった場合には（ステップＣ１４）、ＩＣカード１側の認証で相手端末が不適合するものであるから、この取引きはないものとして処理が終了する。

【０１１２】

なお、端末は、ＩＣカード１から適合応答されると（ステップＴ１５）、取引きを開始するが、不適合であれば、ＩＣカード１との取引きを中止する。

【０１１３】

このように、前処理では、端末とＩＣカード１との両方が相手の適合性を認めない限り、取引きを実施しないため、高いセキュリティを保持した上での電子財布システムを実現することができる。

【０１１４】

つぎに、利用装置４について具体例を用いて説明する。図２１は実施の形態において利用装置の一例である一般取引機の構成例を示すブロック図である。図２１に示した一般取引機は、パチンコ店に設置され、ＩＣカード１を用いたパチンコ玉の排出制御や現金交換等を実施する。

【０１１５】

図２１に示した一般取引機は、ＩＣカードリーダ／ライタ４０１，表示器４０２，テンキー４０３，バーコードリーダ等の機器４０４，レシートプリンタ４０５，ＣＰＵ４０６，メモリ４０７，店舗用カード処理器４０８等により構成される。なお、パチンコ排出や現金交換などの処理そのものは、一般取引機に接続される他の装置（不図示）によって行われるものとする。

【０１１６】

ＩＣカードリーダ／ライタ４０１は、ＩＣカード１を装着してＩＣカード１に記憶されたデータを読み出したり書き込む。表示器４０２は、取引時の情報を可視表示する。テンキー４０３は、ＩＣカード１による支払い額などを入力するための数字キーである。バーコードリーダ等の機器４０４は、バーコードが記録されたシートからバーコードデータを読み取る機器である。レシートプリンタ４０５は、パチンコ玉変換や現金変換等のサービスの結果などを記録する。ＣＰＵ４０６は、この一般取引機全体の処理を制御する。メモリ４０７は、ＣＰＵ４０６が動作するためのプログラムを格納したＲＯＭおよびＣＰＵ４０６のワークエリアとして使用されるＲＡＭよりなる。店舗用カード処理器４０８は、店舗独自のカードを処理する機器である。

【０１１７】

さらに他の例について説明する。図２２は実施の形態において利用装置の一例である一般取引電話機の構成例を示すブロック図である。

【０１１８】

図２２に示した一般取引電話機は、ＩＣカードリーダ／ライタ５０１，表示器５０２，電話機等サービス／度数制御の機器５０３，レシートプリンタ５０４，ＣＰＵ５０５，メモリ５０６，店舗用カード処理器５０７等により構成される。

【０１１９】

ＩＣカードリーダ／ライタ５０１は、ＩＣカード１を装着してＩＣカード１に記憶されたデータを読み出したり書き込む。表示器５０２は、取引時の情報を可視表示する。電話機等サービス／度数制御の機器５０３は、図示せぬ電話回線に接続され、電話機能を果たす際に時間および通話距離等に応じて課金する度数を制御する。レシートプリンタ５０４は、電話サービスの結果などを記録する。ＣＰＵ５０５は、この一般取引電話機全体の処理を制御する。メモリ５０６は、ＣＰＵ５０５が動作するためのプログラムを格納したＲＯＭおよびＣＰＵ５０５のワークエリアとして使用されるＲＡＭよりなる。店舗用カード処理器５０７は、店舗独自のカードを処理する機器である。

【０１２０】

つぎに、利用装置４の動作について説明する。まず、一般取引機の動作について説明する。図２３、図２４および図２５は図２１に示した一般取引機とＩＣカード１間の取引動作を説明するフローチャートである。この一般取引機は領域ＩＤをもたず、機械ＩＤに従って処理を実行する。

【０１２１】

図２１に示した一般取引機は、まず、前処理を実行する（ステップＴ１０１）。この前処理は前述した端末の動作と同様に実施される（図１９および図２０参照）。一方、ＩＣカード１においても、前処理が実行され（ステップＣ１０１）、その処理内容は前述した図１９および図２０に従うものである。

【０１２２】

一般取引機が前処理を終了すると、続いて自身の機械ＩＤが読み出される（ス

テップＴ１０２）。このとき、一般取引機の表示器４０２に支払い要求額の入力を要請する表示画面が形成される。この段階では、支払い要求額の入力が可能となり、以降でその支払い要求額が入力された場合には、その支払い要求額は一時メモリ４０７に格納される。そして、機械ＩＤが支払いコマンドとともにＩＣカード１に送信された後（ステップＴ１０３）、一般取引機は、ＩＣカード１から送られてくる第２財布の金額の受信待ちとなる（ステップＴ１０４）。

【０１２３】

ＩＣカード１は、ＩＤおよび支払いコマンドを受信すると（ステップＣ１０２）、その支払いコマンドに領域ＩＤが含まれているか否かを判断する（ステップＣ１０３）。もし支払いコマンドに領域ＩＤが含まれていた場合には（ステップＣ１０３）、第２ディレクトリＤ２から第２財布アドレスが読み取られ（ステップＣ１０４）、一方、含まれていないかった場合には（ステップＣ１０３）、この取引きは終了する。

【０１２４】

処理がステップＣ１０５に移行した場合には、受信された機械ＩＤが第２ディレクトリＤ２の機械ＩＤと一致するか否か判断される。もし一致する場合には、続くステップＣ１０６において、第２財布アドレスに従って第２財布エリア１０６Ｂから残高が読み出されるとともに、その残高が一般取引機に出力される。

【０１２５】

一般取引機は、ＩＣカード１から第２財布の残高を受信すると（ステップＴ１０５）、その受信額を表示器４０２に表示する（ステップＴ１０６）。そして、この段階ですでにテンキー４０３の操作による支払い要求額の入力がなされていれば（ステップＴ１０７）、処理はステップＴ１１１に移行する。ステップＳ１１１では、メモリ４０７に格納された支払い要求額が読み出され、ＩＣカード１に送信される。その後、処理はステップＴ１１２に移行する。

【０１２６】

一方、支払い要求額が未入力であれば（ステップＴ１０７）、処理は一定時間の入力待ちとなり（ステップＴ１０８）、その支払い要求額はテンキー４０３により入力された段階で（ステップＴ１０９）、そのままＩＣカード１に送信され

る（ステップＴ１１０）。その後、処理はステップＴ１１２に移行する。

【０１２７】

ＩＣカード１は、一般取引機よりすでに支払いコマンドを受信しており（ステップＣ１０７）、さらに支払い要求額を受信する（ステップＣ１０８）。この場合、ＩＣカード１は、第２財布の残高から受信された支払い要求額を差し引いてその結果得られた金額をワークエリアＷ１に格納する（ステップＣ１０９）。

【０１２８】

そして、ワークエリアＷ１の格納額がゼロもしくはプラスであれば（ステップＣ１１０）、支払い可としてその支払い可の情報と支払い額とが一般取引機に通知される（ステップＣ１１１）。この後、処理は受け取りコードの待ち状態となる。一方、ワークエリアＷ１の格納額がマイナスであれば（ステップＣ１１０）、この取引きはなかったものとして処理は終了する。

【０１２９】

一般取引機は、ＩＣカード１より支払い可としての支払い額を受信すると（ステップＴ１１２）、その支払い額を表示器４０２に利用者が確認できるように表示する（ステップＴ１１３）。そして、処理はテンキー４０３に設けられた確認キーの操作による確認待ち状態となる（ステップＴ１１４）。利用者が確認キーを操作した場合には、その確認操作が受け付けられ（ステップＴ１１４）、ＩＣカード１に対して確認応答が送信され（ステップＴ１１５）、さらに支払い額の受信完了を示す受け付けコードが送信される（ステップＴ１１６）。

【０１３０】

ＩＣカード１は、確認応答の受信を一定時間内に受け付けると（ステップＣ１１２）、さらに受け取りコードを受信する（ステップＣ１１４）。なお、一定時間内に確認応答が受け付けられなかった場合には、この取引きはなかったものとしてワークエリアＷ１はクリアされ（ステップＣ１１３）、処理が終了する。

【０１３１】

ステップＣ１１４において受け取りコードが受信された後、処理はステップＣ１１５に移行して、ワークエリアＷ１の格納額を第２財布エリア１０６Ｂに格納する。これによりサービスと交換に支払う金額分が第２財布から取り出されるこ

とになる。そして、第３財布エリア１０６Ｃには、この取引きの履歴（日付など）が格納され（ステップＣ１１６）、最後に取引完了署名コードが一般取引機に送信される（ステップＣ１１７）。

【０１３２】

一般取引機は、ＩＣカード１から取引完了署名コードを受信すると、自己取引履歴の作成および残高更新を行って（ステップＴ１１７）、サービス処理（パチンコ玉排出制御，現金交換等）を実行する（ステップＴ１１８）。最後に、ＩＣカード１がＩＣカードリーダ／ライタ４０１から返却される（ステップＴ１１９）。

【０１３３】

続いて、一般取引電話機の動作について説明する。図２６、図２７および図２８は図２２に示した一般取引電話機とＩＣカード１間の取引動作を説明するフローチャートである。

【０１３４】

図２２に示した一般取引電話機は、まず、前処理を実行する（ステップＴ２０１）。この前処理は前述した端末の動作と同様に実施される（図１９および図２０参照）。一方、ＩＣカード１においても、前処理が実行され（ステップＣ２０１）、その処理内容は前述した図１９および図２０に従うものである。

【０１３５】

一般取引電話機が前処理を終了すると、続いて自身の機械ＩＤが読み出される（ステップＴ２０２）。このとき、一般取引電話機の表示器５０２に支払い要求額の入力を要請する表示画面が形成される。この段階では、支払い要求額の入力が可能となり、以降でその支払い要求額が入力された場合には、その支払い要求額は一時メモリ５０６に格納される。そして、機械ＩＤが支払いコマンドとともにＩＣカード１に送信された後（ステップＴ２０３）、一般取引電話機は、ＩＣカード１から送られてくる第２財布の金額の受信待ちとなる（ステップＴ２０４）。

【０１３６】

ＩＣカード１は、ＩＤおよび支払いコマンドを受信すると（ステップＣ２０２

）、その支払いコマンドに領域ＩＤが含まれているか否かを判断する（ステップＣ２０３）。もし支払いコマンドに領域ＩＤが含まれていた場合には（ステップＣ２０３）、第２ディレクトリＤ２から第２財布アドレスが読み取られ（ステップＣ２０４）、一方、含まれていないかった場合には（ステップＣ２０３）、この取引きは終了する。

【０１３７】

処理がステップＣ２０５に移行した場合には、受信された機械ＩＤが第２ディレクトリＤ２の機械ＩＤと一致するか否か判断される。もし一致する場合には、続くステップＣ２０６において、第２財布アドレスに従って第２財布エリア１０６Ｂから残高が読み出されるとともに、その残高が一般取引電話機に出力される。

【０１３８】

一般取引電話機は、ＩＣカード１から第２財布の残高を受信すると（ステップＴ２０５）、その受信額を表示器５０２に表示する（ステップＴ２０６）。この後、一般取引電話機では、電話機能のサービスが開始される。

【０１３９】

一般取引電話機は、サービス開始後、通話に応じて単位サービス額を検知するとともに度数制御に従う金額カウンタを更新する（ステップＴ２０７）。そして、第２財布の残金すなわち表示器５０２に表示されている表示額（受信額）から刻々更新される金額カウンタの値が差し引かれ、その結果得られる使用可能金額がゼロに達するまで（ステップＴ２０８）、もしくは、サービスの終了が検知されるまでは（ステップＴ２１０）、ステップＴ２０７における金額カウンタの更新，ステップＴ２０８における使用可能金額の算出およびステップＴ２０９における使用可能金額の表示（表示器５０２の表示ワークエリアへの表示）が実行される。

【０１４０】

そして、使用可能金額がゼロとなった場合（ステップＴ２０８）、もしくはサービスの終了が検知された場合（ステップＴ２１０）、処理はステップＴ２１１に移行して、支払い額の請求が受信されるのを待つ（ステップＴ２１１）。この

ようにして支払額の請求が受信されると（ステップＴ２１１）、金額カウンタの値が読み出され、その値が支払い要求額としてＩＣカード１に送信される（ステップＴ２１２）。

【０１４１】

ＩＣカード１は、一般取引電話機よりすでに支払いコマンドを受信しており（ステップＣ２０７）、さらに支払い要求額を受信する（ステップＣ２０８）。この場合、ＩＣカード１は、第２財布の残高から受信された支払い要求額を差し引いてその結果得られた金額をワークエリアＷ１に格納する（ステップＣ２０９）。

【０１４２】

そして、ワークエリアＷ１の格納額がゼロもしくはプラスであれば（ステップＣ２１０）、支払い可としてその支払い可の情報と支払い額とが一般取引電話機に通知される（ステップＣ２１１）。この後、処理は受け取りコードの待ち状態となる。一方、ワークエリアＷ１の格納額がマイナスであれば（ステップＣ２１０）、この取引きはなかったものとして処理は終了する。

【０１４３】

一般取引電話機は、ＩＣカード１より支払い可としての支払い額を受信すると（ステップＴ２１３）、その支払い額を表示器５０２に利用者が確認できるように表示する（ステップＴ２１４）。そして、処理は電話機等サービス／度数制御の機器５０３に設けられた確認キーの操作による確認待ち状態となる（ステップＴ２１５）。利用者が確認キーを操作した場合には、その確認操作が受け付けられ（ステップＴ２１５）、ＩＣカード１に対して確認応答が送信され（ステップＴ２１６）、さらに支払い額の受信完了を示す受け付けコードが送信される（ステップＴ２１７）。

【０１４４】

ＩＣカード１は、確認応答の受信を一定時間内に受け付けると（ステップＣ２１２）、さらに受け取りコードを受信する（ステップＣ２１４）。なお、一定時間内に確認応答が受け付けられなかった場合には、この取引きはなかったものとしてワークエリアＷ１はクリアされ（ステップＣ２１３）、処理が終了する。

【０１４５】

ステップＣ２１４において受け取りコードが受信された後、処理はステップＣ２１５に移行して、ワークエリアＷ１の格納額を第２財布エリア１０６Ｂに格納する。これによりサービスと交換に支払う金額分が第２財布から取り出されることになる。そして、第３財布エリア１０６Ｃには、この取引きの履歴（日付など）が格納され（ステップＣ２１６）、最後に取引完了署名コードが一般取引機に送信される（ステップＣ２１７）。

【０１４６】

一般取引電話機は、ＩＣカード１から取引完了署名コードを受信すると、自己取引履歴の作成，残高更新およびレシート印刷を行い（ステップＴ２１８）、最後に、ＩＣカード１をＩＣカードリーダ／ライタ５０１から返却する（ステップＴ２１９）。

【０１４７】

つぎに、引出装置２の動作について説明する。図２９～図３２は実施の形態において引出装置とＩＣカード間の取引動作を説明するフローチャートであり、図３３は実施の形態において引出装置による取引動作時の表示画面の一例を示す図である。

【０１４８】

図２９～図３２に示したフローチャートは、引出装置２が預金引出機の例を示している。引出装置２は、まず、ＩＣカード１との引出し取引きを行うため、表示画面に取引金額入力，暗証番号，カード挿入指示を提示する（ステップＴ３０１）。この提示の後、引出装置２は前処理に入る（ステップＴ３０２）。これに伴ってＩＣカード１も前処理を実行する（ステップＣ３０１）。

【０１４９】

続いて、引出装置２は、金額入力および暗証番号入力を経た後（ステップＴ３０３）、支払いコマンドに機械ＩＤおよび領域ＩＤ（第１財布の指定）を含めて送信する（ステップＴ３０４）。

【０１５０】

ＩＣカード１は、引出装置２より支払いコマンドを受信すると（ステップＣ３

０２）、その受信された支払いコマンドに領域ＩＤが含まれることから（ステップＣ３０３）、領域ＩＤの領域を読み取る（ステップＣ３０４）。

【０１５１】

ＩＣカード１は、支払いコマンド中の機械ＩＤを読み出してその機械ＩＤと第１ディレクトリＤ１の機械ＩＤと比較する。そのとき、両機械ＩＤが一致すれば（ステップＣ３０５）、さらにその機械ＩＤのアクセス権と受信アクセスとの対応を確認する（ステップＣ３０６）。なお、機械ＩＤの不一致が確認されると（ステップＣ３０５）、この引出し取引きはなかったものとして無効にされる。

【０１５２】

ステップＣ３０６において対応関係が確認されると、処理はさらにステップＣ３０７に移行する。ステップＣ３０７では、ステップＣ３０４で読み取られた領域が第１財布であれば、処理はステップＣ３０８に移行し、そうでなければ、処理は他モードを実行する。

【０１５３】

処理がステップＣ３０８に移行すると、引出装置２の要求内容を判別する。この場合には、引出装置２が支払いコマンドを送信していることから、要求は支払いと判別される。したがって、ここでは、支払いについてのみ図示（図２９、図３０および図３１参照）およびその説明を詳述し、他の転送，カード預金などは、前述したＩＣカード１の動作に従うものとする。

【０１５４】

さて、支払い要求の場合には、すでに説明した図１２および図１３の支払い処理が開始される。この支払い処理では、まず、引出装置２に対して暗証番号および要求額が要請される（ステップＣ３０９）。

【０１５５】

引出装置２は、ＩＣカード１より暗証番号と支払い額との要請を受け付けると、その両情報が入力済みであるか判断する（ステップＴ３０５）。この場合、ステップＴ３０３において両情報はすでに入力済みであることから、処理はつぎのステップＴ３０６に移行する。ステップＴ３０６において両情報すなわち暗証番号と支払い額とが暗号化され、続くステップＴ３０７においてこれら暗号化情報

はＩＣカード１に送信される。

【０１５６】

ＩＣカード１は、その後、暗証番号および支払い要求額を受信すると（ステップＣ３１０）、まず暗証番号を復号する（ステップＣ３１１）。このようにして暗証番号が復号されると、続くステップＣ３１２において、第１ディレクトリＤ１に格納されている暗証番号が読み出され、その暗証番号が復号される。

【０１５７】

さらに、この復号されたＩＣカード１自身の暗証番号と取引装置２から受け取って復号した暗証番号との照合が行われ（ステップＣ３１３）、両暗証番号が一致した場合には（ステップＣ３１４）、認証をパスできたものとして処理はステップＣ３１５に移行する。一方、認証をパスできなかった場合には、この支払い取引きはなかったものとして無効にされる。

【０１５８】

さらに、ＩＣカード１では、第１財布エリア１０６Ａおよび第２財布エリア１０６Ｂの各残高が暗号化して引出装置２に送信される（ステップＣ３１５）。これにより、引出装置２は、ＩＣカード１から第１財布，第２財布の各残高を受信すると（ステップＴ３０８）、残高表示を行って利用者に第１財布と第２財布の残り金額を提示する（ステップＴ３０９）。その後、引出装置２はＩＣカード１からの支払い可の通知を待つ（ステップＴ３１０）。

【０１５９】

ＩＣカード１では、受信された支払い要求額が復号される（ステップＣ３１６）。その後、第１財布エリア１０６Ａに格納された残高から復号された支払い要求額が差し引かされ、その金額がワークエリアＷ２に格納される（ステップＣ３１７）。

【０１６０】

そして、ワークエリアＷ２に格納された金額がゼロもしくはプラスであった場合には（ステップＣ３１８）、支払い可となることからその支払い可の情報，第１財布の残高およびワークエリアＷ２に格納された金額がそれぞれ暗号化される（ステップＣ３２２）。このようにして暗号化された各情報は暗号化情報として

引出装置２に送信される（ステップＣ３２３）。一方、ワークエリアＷ２に格納された金額がマイナスであった場合には（ステップＣ３１８）、処理はステップＣ３１９に移行して図１４に示した追加取引を実行する。

【０１６１】

すなわち、ＩＣカード１はさらに第２財布エリア１０６Ｂから残高を読み取り（ステップＣ３１９）、その金額をワークエリアＷ２の格納額に加算してその合計をワークエリアＷ２の格納額とする（ステップＣ３２０）。この後に、再度ワークエリアＷ２の格納額がゼロもしくはプラスに転じていれば、ＩＣカード１は上述したステップＣ３２２およびステップＣ３２３において支払い可，第１財布の残高およびワークエリアＷ２の格納額の暗号化および送信を実行する。

【０１６２】

引出装置２は、ＩＣカード１から暗号化情報を受信して支払い可を確認すると（ステップＴ３１０）、図３３に示したように、ワークエリアＷ２の金額から支払い前後の残高確認表示を行う（ステップＴ３１１）。

【０１６３】

この残高確認表示では、第１財布，第２財布それぞれの支払い前と支払い後の金額（一例として円表示）が表示され、さらに支払い額、確認操作のためのアイコン「確認」および取り消し操作のためのアイコン「取消」が表示される。これらの操作は図示せぬキー操作パネルによって行われる。図３３の例では、第１財布の支払い前後の金額はそれぞれａ円，Ａ円となり、第２財布の支払い前後の金額はそれぞれｂ円，Ｂ円となる。さらに、支払い額はＣ円となる。

【０１６４】

そして、引出装置２は利用者による確認操作を待ち（ステップＴ３１２）、その確認操作を受け付けると同時にＩＣカード１に対して確認応答の送信（ステップＴ３１３）および受け取りコードの送信を行う（ステップＴ３１４）。ここで、受け取りコードとは、確かにＩＣカード１より支払いを受けたということを証明するものである。

【０１６５】

ＩＣカード１において、ステップＣ３２３の暗号化送信の後、引出装置２から

一定時間内に応答受信がない場合には（ステップＣ３２４）、処理はステップＣ３２５に移行して、この支払い取引きはなかったものにするため、ワークエリアＷ２はクリアされる。一方、ステップＣ３２４において応答受信が確認された場合には、その応答受信によって受信されたデータが受け取りコードか否か判断される（ステップＣ３２６）。

【０１６６】

受信データが受け取りコードであった場合には、支払い取引きが成立したものとして、ワークエリアＷ２の暗号化された金額が第１財布エリア１０６Ａに格納される（ステップＣ３２７）。このようにして、第１財布エリア１０６Ａは、支払い要求金額に従って残高が更新される。

【０１６７】

さらに、第３財布エリア１０６Ｃには、上述した転送取引きの日付などの情報が履歴として格納される（ステップＣ３２８）。最後に、取引装置２に対してＩＣカード１内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップＣ３２９）。

【０１６８】

引出装置２は、ＩＣカード１から取引完了署名コードを受け取ると、自己取引履歴を作成して自己のＩＣカードに記録するとともに、残高更新およびレシート印刷を行った後に処理を終了する（ステップＴ３１５）。

【０１６９】

つぎに、引出装置２の応用例を用いて説明する。図３４は実施の形態において引出装置の一例であるＡＴＭ（Ａｕｔｏｍａｔｉｃ　Ｔｅｌｌｅｒ　Ｍａｃｈｉｎｅ）機の構成例を示すブロック図である。

【０１７０】

図３４に示したＡＴＭ機は、ＣＲＴ／タッチパネル６０１，表示制御部６０２，入力検知部６０３，ＩＣカードリーダ／ライタ６０４，インタフェース６０５，キャッシュカウンタ／預金機構６０６，機構制御部６０７，回線制御部６０８，暗号化／復号化ボード６０９，ＣＰＵ６１０，メモリ６１１，外部メモリ６１２，銀行用ＩＣカードリーダ６１３などにより構成される。

【0171】

ＣＲＴ／タッチパネル６０１は、表示画面をタッチしてデータや各種の操作を入力する。表示制御部６０２は、ＣＲＴ／タッチパネル６０１のＣＲＴ表示を制御し、入力検知部６０３は、ＣＲＴ／タッチパネル６０１のタッチ入力を検知する。ＩＣカードリーダ／ライタ６０４は、ＩＣカード１を装着してデータの読み出しや書き込みを行う。インタフェース６０５は、ＩＣカード１とＡＴＭ機内部とのインタフェースを司る。

【0172】

キャッシュカウンタ／預金機構６０６は、金額をカウントして支払うキャッシュカウンタと金額をカウントして口座に入金する制御機構である。機構制御部６０７は、キャッシュカウンタ／預金機構６０６を制御する。回線制御部６０８は、回線を介してセンタシステム３のホストコンピュータ３１と通信を制御する。暗号化／復号化ボード６０９は、取引き時におけるデータの暗号化および復号化を行う。

【0173】

ＣＰＵ６１０は、装置全体を制御する。メモリ６１１はＣＰＵ６１０が動作するためのプログラムを格納したＲＯＭおよびＣＰＵ６１０のワークエリアとして使用するＲＡＭにより構成される。外部メモリ６１２は、ハードディスクなどの大容量メモリである。銀行用ＩＣカードリーダ６１３は、オンラインバンキングの手続きを行うための通常の銀行カードを装着して認証情報を読み出す。

【0174】

つぎに、ＡＴＭ機の動作について説明する。図３５～図３７は図３４に示したＡＴＭ機とＩＣカード間の取引動作を説明するフローチャートであり、図３８および図３９は実施の形態においてＡＴＭ機による取引動作時の表示画面の一例を示す図である。

【0175】

ＡＴＭ機は、まず、ＩＣカード１との引出し取引きを行うため、図３８（ａ）に示したように、ＣＲＴ／タッチパネル６０１に、カード挿入指示，暗証番号入力，モード入力を提示した初期画面を形成する（ステップＴ４０１）。この初期

画面形成後、ＡＴＭ機は前処理に入る（ステップＴ４０２）。これに伴ってＩＣカード１も前処理を実行する（ステップＣ４０１）。

【０１７６】

続いて、ＡＴＭ機は、カード挿入指示を消去するなどして第２画面を表示する（ステップＴ４０３）。その後、ＣＲＴ／タッチパネル６０１へのタッチ操作によりモード（支払い，預金（カード預金），振込，残高照会）指定が行われると（ステップＴ４０４）、その指定モードがいずれであるのか判断される（ステップＴ４０５）。ここでは、支払いモードについての例を挙げる。したがって、支払いモード以外のモードが指定された場合には、他のモード処理として図示および説明を省略する。

【０１７７】

なお、他のモードとして、預金モードが指定された場合には、図３８（ｃ）に示した預金モード画面のように、さらに細かいモードとして現金からＩＣカードへのモードと現金を口座へ移すモードとが用意される。また、振込モードが指定された場合には、図３８（ｄ）に示した振込モード画面のように、さらに細かいモードとしてＩＣカードから振込先へのモードと口座から振込先へのモードとが用意される。また、残高照会モードが指定された場合には、図３８（ｅ）に示したように、さらに細かい指定として口座預金残高，口座とＩＣカードとの両残高，ＩＣカード残高の３つが用意される。

【０１７８】

さて、支払いモードが指定された場合には（ステップＴ４０５）、図３８（ｂ）に示したように、ＣＲＴ／タッチパネル６０１に、支払いモード画面が形成される（ステップＴ４０６）。そして、この支払いモード画面についても、さらに細かくモード指定が行われる。

【０１７９】

すなわち、支払いモード画面には、口座からＩＣカードへ、口座から現金へ、ＩＣカードからＩＣカードへ、ＩＣカードから現金へ、口座からＩＣカードおよび現金へ、ＩＣカードからＩＣカードおよび現金への６種類のモードが用意される（図３８（ｂ）～（ｅ）では、ＩＣカードを省略してカードで示している）。

利用者はこれら６種類のモードから所要のモードをタッチ操作により指定する。ここでは、口座からＩＣカード１へのモードが指定された場合を例に挙げ、その他のモードについては他のモード処理として図示および説明を省略する。

【０１８０】

口座／カードモードが指定された場合には、ＣＲＴ／タッチパネル６０１に図３９（ａ）に示した金額指定画面が表示され、その金額指定画面に対する操作および画面編集が行われる（ステップＴ４０９）。図３９（ａ）に示した金額指定画面は、Ａ１（仮の一方）からＡ２（仮の他方）へ引き落とす金額を入力する旨の指示、金額を入力するための数字キー、金額の単位（一例として“万円”，“千円”）を入力するためのキー、金額入力後の確認キー、このモードを取り消すための取消キーが表示される。いずれの表示も、タッチ入力が可能である。

【０１８１】

ここで、指定されたモードが口座／カードモードであることから、Ａ１には“口座”が設定され、Ａ２には“カード”（ＩＣカード１の意味）が設定される（ステップＴ４１０）。そして、図３９（ａ）の金額指定画面において処理は金額の指定待ちとなる（ステップＴ４１１）。その後、金額指定があると（ステップＴ４１１）、処理はさらに暗証番号の入力待ちとなる（ステップＴ４１２）。

【０１８２】

ＡＴＭ機は、このようにして金額指定および暗証番号入力を経た後（ステップＴ４１１およびステップＴ４１２）、更新コマンドに暗証番号，支払い要求額（金額指定された額），機械ＩＤ，領域ＩＤ（ここでは第１財布の指定）を含めた暗号化送信を行う（ステップＴ４１３）。なお、更新コマンドとしたのは、Ａ１からＡ２への金額の移動でＡ１とＡ２の残高が更新されるためである。ただし、この更新コマンドは、ステップＴ４０５で指定したモードを特定する内容となる。

【０１８３】

ＩＣカード１は、ＡＴＭ機より支払いコマンドを受信すると（ステップＣ４０２）、その受信された更新コマンドに領域ＩＤが含まれることから（ステップＣ４０３）、領域ＩＤの領域を読み取る（ステップＣ４０４）。

【０１８４】

ＩＣカード１は、更新コマンド中の機械ＩＤを読み出してその機械ＩＤと第１ディレクトリＤ１の機械ＩＤと比較する。そのとき、両機械ＩＤが一致すれば（ステップＣ４０５）、さらにその機械ＩＤのアクセス権と受信アクセスとの対応を確認する（ステップＣ４０６）。なお、機械ＩＤの不一致が確認されると（ステップＣ４０５）、この引出し取引きはなかったものとして無効にされる。

【０１８５】

ステップＣ４０６において対応関係が確認されると、処理はさらにステップＣ４０７に移行する。ステップＣ４０７では、ステップＣ４０４で読み取られた領域が第１財布であれば、処理はステップＣ４０８に移行し、そうでなければ、処理はステップＣ４１２に移行してさらにモード指定が支払いモードか否かを確認する。

【０１８６】

ＩＣカード１において、処理がステップＣ４０８に移行した場合には、領域ＩＤが第３財布すなわちセンタ口座情報を指定しているか否かを判断する。上述の流れでは、第１財布のため、この場合にもこの取引きはなかったものとして処理は終了する。なお、第３財布の指定であった場合には、処理はさらにステップＣ４０９に移行してセンタ口座情報のアクセス権を確認する。そこで、ＡＴＭ機が読み出しできる機械であった場合には（ステップＣ４０９）、続くステップＣ４１０において口座番号が読み出され、その口座番号がＡＴＭ機に出力される（ステップＣ４１１）。その後、この取引は終了する。

【０１８７】

ステップＣ４０７において領域ＩＤが第１財布を指定していた場合には、処理はステップＣ４１２に移行するので、そこで要求内容が判別される。上述の流れでは、要求は支払いと判別される。したがって、ここでは、支払いについてのみ図示（図２９、図３０および図３１参照）およびその説明を詳述し、他の転送，カード預金などは、前述したＩＣカード１の動作に従うものとする。

【０１８８】

さて、支払い要求の場合には、すでに説明した図１２および図１３の支払い処

理が開始される。ＩＣカード１は、すでにステップＣ４０１において暗証番号および支払い要求額を受信している。したがって、まず、暗証番号が復号され（ステップＣ４１３）、続くステップＣ４１４において、第１ディレクトリＤ１に格納されている暗証番号が読み出され、その暗証番号が復号される。

【０１８９】

さらに、この復号されたＩＣカード１自身の暗証番号とＡＴＭ機から受け取って復号した暗証番号との照合が行われ（ステップＣ４１５）、両暗証番号が一致した場合には（ステップＣ４１６）、認証をパスできたものとして処理はステップＣ４１７に移行する。一方、認証をパスできなかった場合には、この支払い取引きはなかったものとして無効にされる。

【０１９０】

さらに、ＩＣカード１は、第１財布エリア１０６Ａおよび第２財布エリア１０６Ｂの各残高を暗号化してからＡＴＭ機に送信する（ステップＣ４１７）。

【０１９１】

ＡＴＭ機は、ステップＴ４１３による暗号化送信の後、ＩＣカード１からの第１財布，第２財布の各残高（暗号化情報）の受信待ちとなる（ステップＴ４１４）。その待ち時間が一定時間を経過すると、処理は強制的にカード返却に移行して終了する。

【０１９２】

ＡＴＭ機において、一定時間内にＩＣカード１から第１財布，第２財布の各残高（暗号化情報）が受信されると（ステップＴ４１４）、まず、暗証番号，口座情報，引き落とし額（支払い額）がセンタシステム３に送信される（ステップＴ４１６）。なお、口座情報については、上述したステップＣ４０８～ステップＣ４１１をＩＣカード１に実行させることで取得することができる。続いて、その受信された各残高は図３９（ｂ）に示したように、ＣＲＴ／タッチパネル６０１に表示される（ステップＴ４１７）。その後、ＡＴＭ機はセンタシステム３からの支払い可の通知を待つ（ステップＴ４１９）。

【０１９３】

ＩＣカード１は、ステップＣ４１７において暗号化情報を送信した後、すでに

受信された支払い要求額を復号する（ステップＣ４１８）。その後、第１財布エリア１０６Ａに格納された残高にその復号された支払い要求額が加算され、その金額がワークエリアＷ２に格納される（ステップＣ４１９）。そして、処理はＡＴＭ機からの確認コードの受信待ちとなる（ステップＣ４２０）。

【０１９４】

ＡＴＭ機は、センタシステム３より支払い可の通知を受け取ると（ステップＴ４１８）、利用者による確認操作に従って（ステップＴ４１９）、ＩＣカード１に対して確認コードを送信する（ステップＴ４２０）。この後に、ＩＣカード１より取引完了署名コードが受信されると、履歴などの処理を経てＡＴＭ機側の処理が終了する。

【０１９５】

ＩＣカード１において、ＡＴＭ機から確認コードが受信された場合には（ステップＣ４２０）、支払い取引きが成立したものとして、ワークエリアＷ２の暗号化された金額が第１財布エリア１０６Ａに格納される（ステップＣ４２１）。このようにして、第１財布エリア１０６Ａは、口座からＩＣカードへの支払い要求金額に従って残高が更新される。

【０１９６】

さらに、第３財布エリア１０６Ｃには、上述した転送取引きの日付などの情報が履歴として格納される（ステップＣ４２２）。最後に、ＡＴＭ機に対してＩＣカード１内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップＣ４２３）。

【０１９７】

さて、上述した処理は、口座からＩＣカード１への支払いモードを例に挙げているが、その他に、例えば、口座からＩＣカードおよび現金へ、もしくは、ＩＣカードからＩＣカードおよび現金への支払いであれば、図３９（ｃ）の如く表示画面が形成される。この場合には、支払先となる財布（例えば第２財布でも可）や現金について、それぞれ引き落としたい金額を指定することができる。

【０１９８】

また、図３９（ｂ）には、財布の残高を表示させるだけであったが、図３９（

d）のように、取引完了後の口座残高についても表示するようにしてもよい。

【0199】

以上説明したように、この実施の形態によれば、二重財布（ＩＣカード）としての特性が生かされ、セキュリティの低い方の第２財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の第１財布についてはさらにセキュリティを向上させることが可能である。

【0200】

また、利用装置が領域指定せずに支払い処理を要求した場合には、第２財布の預金額を用いて、セキュリティの低い、個人認証を伴わない簡易な利用取引きを実現することが可能である。

【0201】

また、ＩＣカード１により、セキュリティの低い第２財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第１財布については個人認証や暗号利用により不正防止を図ることが可能である。

【0202】

また、取引装置とＩＣカードとの取引きで、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引きについてはモードによるバリエーションを持たせ、現金での取引きについてはその指定操作を省くことで、現金取引きの簡略化を実現することが可能である。

【0203】

また、取引装置とＩＣカードとの個人認証を要する取引きで、第１財布だけで金額上の取引きが成立しなくても第２財布の金額を補填して再度取引きを遂行するようにしたので、利用者が取引きのための金額を気にすることなく取引きを遂行することができ、操作性の向上を図ることが可能である。

【0204】

また、取引装置とＩＣカードとの取引きで、個人認証を経た場合にのみ第１財布および第２財布の金額を取引装置に出力し、そうでない場合には第２財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に

教える程度の取引きであっても、個人認証を通過できなければセキュリティの高い第１財布を開くことを防止することが可能である。

【０２０５】

以上、この発明を実施の形態により説明したが、この発明の主旨の範囲内で種々の変形が可能であり、これらをこの発明の範囲から排除するものではない。

【０２０６】

【発明の効果】

以上説明したように、請求項１の発明によれば、二重財布（ＩＣカード）としての特性が生かされ、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能な二重財布を有する電子財布システムが得られるという効果を奏する。

【０２０７】

また、請求項１の発明は、請求項２のように、カード状担体の第２不揮発性メモリに第２領域が引出処理のみ許容するプログラムを格納するようにしてもよい。

【０２０８】

また、請求項１の発明は、請求項３の発明のように、カード状担体に設けた第３領域に当該第３領域へのアクセスを許容する利用装置の識別情報および暗証番号を登録しておき、利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に第３領域の加算又は減算を許容するようにしてもよい。

【０２０９】

また、請求項３の発明は、請求項４の発明のように、カード状担体の第３領域に、加算処理した利用装置を示す識別情報と加算処理した額とを履歴情報として格納するようにしてもよい。

【０２１０】

また、請求項５の発明によれば、利用装置が領域指定せずに支払い処理を要求した場合には、第２領域の預金額を用いて、セキュリティの低い、個人認証を伴

わない簡易な利用取引きを実現することが可能な二重財布を有する電子財布システムが得られるという効果を奏する。

【0211】

また、請求項6の発明によれば、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については個人認証により不正防止を図ることが可能な二重財布を有する電子財布システムに適用されるICカードが得られるという効果を奏する。

【0212】

また、請求項7の発明によれば、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については暗号利用により不正防止機能を一層向上させることが可能な二重財布を有する電子財布システムに適用されるICカードが得られるという効果を奏する。

【0213】

また、請求項8によれば、取引装置とICカードとの取引きで、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引きについてはモードによるバリエーションを持たせ、現金での取引きについてはその指定操作を省くことで、現金取引きの簡略化を実現することが可能なICカード取引装置が得られるという効果を奏する。

【0214】

また、請求項9の発明によれば、取引装置とICカードとの個人認証を要する取引きで、第1財布だけで金額上の取引きが成立しなくても第2財布の金額を補填して再度取引きを遂行するようにしたので、利用者が取引きのための金額を気にすることなく取引きを遂行することができ、操作性の向上を図ることが可能なICカード取引装置が得られるという効果を奏する。

【0215】

また、請求項10の発明によれば、取引装置とICカードとの取引きで、個人認証を経た場合にのみ第1財布および第2財布の金額を取引装置に出力し、そう

でない場合には第２財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に教える程度の取引きであっても、個人認証を通過できなければセキュリティの高い第１財布を開くことを防止することが可能なＩＣカード取引システムに適用されるＩＣカードが得られるという効果を奏する。

【図面の簡単な説明】

【図１】

この発明に係る実施の形態による電子財布システムの一例を示す構成図である。

【図２】

図１に示したＩＣカードを機能的に示すブロック図である。

【図３】

図１に示したＩＣカードをハードウェア的に示すブロック図である。

【図４】

図３に示したＩＣカードのメモリ構成例を示す図である。

【図５】

図１に示した引出装置を機能的に示すブロック図である。

【図６】

図１に示したセンタシステムを概略的に示す構成図である。

【図７】

図１に示した利用装置を機能的に示すブロック図である。

【図８】

この発明に係る実施の形態によるＩＣカードのメイン動作を説明するフローチャートである。

【図９】

この発明に係る実施の形態によるＩＣカードのメイン動作を説明するフローチャートである。

【図１０】

図８に示したメイン動作における転送処理を説明するフローチャートである。

【図１１】

図８に示したメイン動作における転送処理を説明するフローチャートである。

【図１２】

図８に示したメイン動作における支払い処理を説明するフローチャートである。

【図１３】

図８に示したメイン動作における支払い処理を説明するフローチャートである。

【図１４】

図１１に示した支払い処理における追加取引を説明するフローチャートである。

【図１５】

図８に示したメイン動作におけるカード預金処理を説明するフローチャートである。

【図１６】

図８に示したメイン動作におけるカード預金処理を説明するフローチャートである。

【図１７】

この発明に係る実施の形態における復号処理を説明するフローチャートである。

【図１８】

この発明に係る実施の形態における暗号化処理を説明するフローチャートである。

【図１９】

この発明に係る実施の形態における前処理を説明するフローチャートである。

【図２０】

この発明に係る実施の形態における前処理を説明するフローチャートである。

【図２１】

この発明に係る実施の形態において利用装置の一例である一般取引機の構成例を示すブロック図である。

【図２２】

この発明に係る実施の形態において利用装置の一例である一般取引電話機の構成例を示すブロック図である。

【図２３】

図１８に示した一般取引機とＩＣカード間の取引動作を説明するフローチャートである。

【図２４】

図１８に示した一般取引機とＩＣカード間の取引動作を説明するフローチャートである。

【図２５】

図１８に示した一般取引機とＩＣカード間の取引動作を説明するフローチャートである。

【図２６】

図１９に示した一般取引電話機とＩＣカード間の取引動作を説明するフローチャートである。

【図２７】

図１９に示した一般取引電話機とＩＣカード間の取引動作を説明するフローチャートである。

【図２８】

図１９に示した一般取引電話機とＩＣカード間の取引動作を説明するフローチャートである。

【図２９】

この発明に係る実施の形態において引出装置とＩＣカード間の取引動作を説明するフローチャートである。

【図３０】

この発明に係る実施の形態において引出装置とＩＣカード間の取引動作を説明するフローチャートである。

【図３１】

この発明に係る実施の形態において引出装置とＩＣカード間の取引動作を説明

するフローチャートである。

【図３２】

この発明に係る実施の形態において引出装置とＩＣカード間の取引動作を説明するフローチャートである。

【図３３】

この発明に係る実施の形態において引出装置による取引動作時の表示画面の一例を示す図である。

【図３４】

この発明に係る実施の形態において引出装置の一例であるＡＴＭ機の構成例を示すブロック図である。

【図３５】

図２８に示したＡＴＭ機とＩＣカード間の取引動作を説明するフローチャートである。

【図３６】

図２８に示したＡＴＭ機とＩＣカード間の取引動作を説明するフローチャートである。

【図３７】

図２８に示したＡＴＭ機とＩＣカード間の取引動作を説明するフローチャートである。

【図３８】

この発明に係る実施の形態においてＡＴＭ機による取引動作時の表示画面の一例を示す図である。

【図３９】

この発明に係る実施の形態においてＡＴＭ機による取引動作時の表示画面の一例を示す図である。

【符号の説明】

１　ＩＣカード

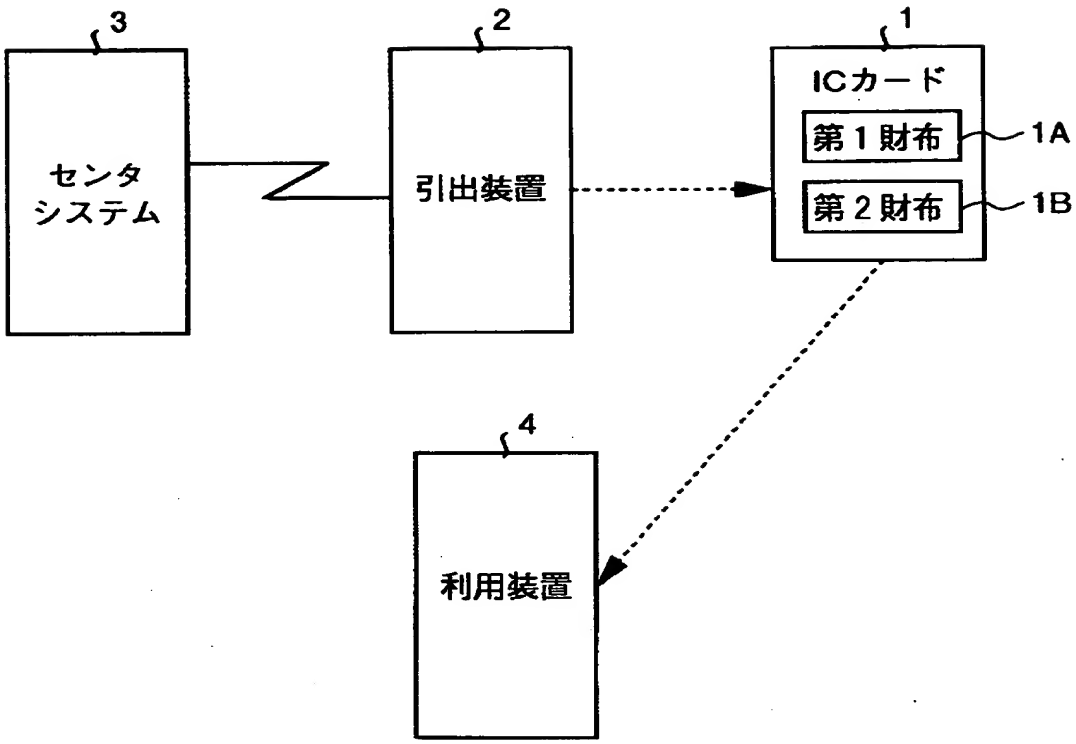
２　引出装置

３　センタシステム

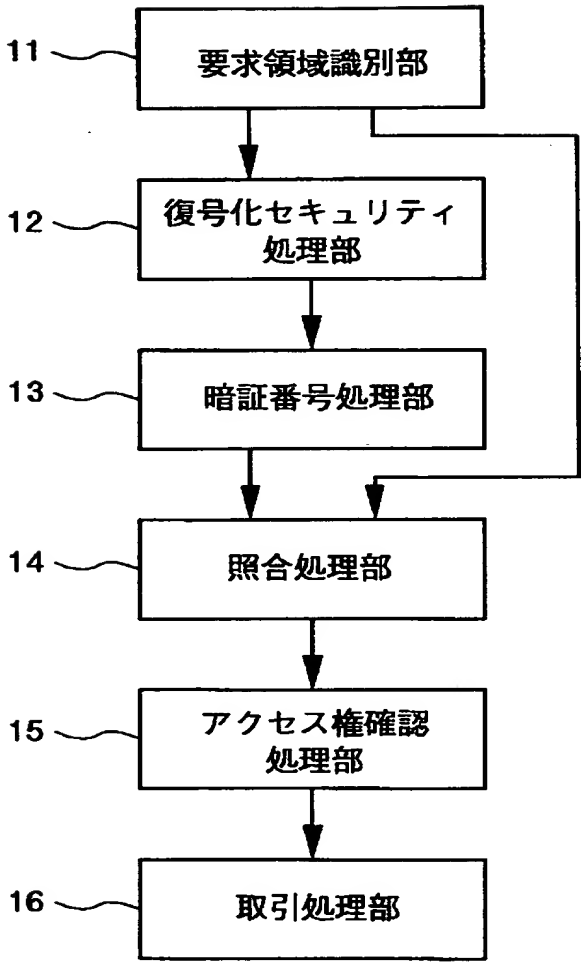
４　利用装置
１１　要求領域識別部
１２　復号化セキュリティ処理部
１３　暗証番号処理部
１４　照合処理部
１５　アクセス権確認処理部
１６　取引処理部
２１　機械ＩＤレジスタ
２２　認証転送処理部
２３　暗号化処理部
３１　ホストコンピュータ
３２　データベース
４１　機械ＩＤレジスタ
４２　転送処理部
４３　支払い額発生部
４４　取引処理部
４５　受信部
４６　メモリ
１０３　ＣＰＵ
１０４　ＲＯＭ
１０５　ＲＡＭ
１０６　ＥＥＰＲＯＭ
１０６Ａ　第１財布エリア
１０６Ｂ　第２財布エリア
１０６Ｃ　第３財布エリア
４０１，５０１，６０４　ＩＣカードリーダ／ライタ
４０６，５０５，５１０　ＣＰＵ
４０７，５０６，６１１　メモリ

【書類名】　図面

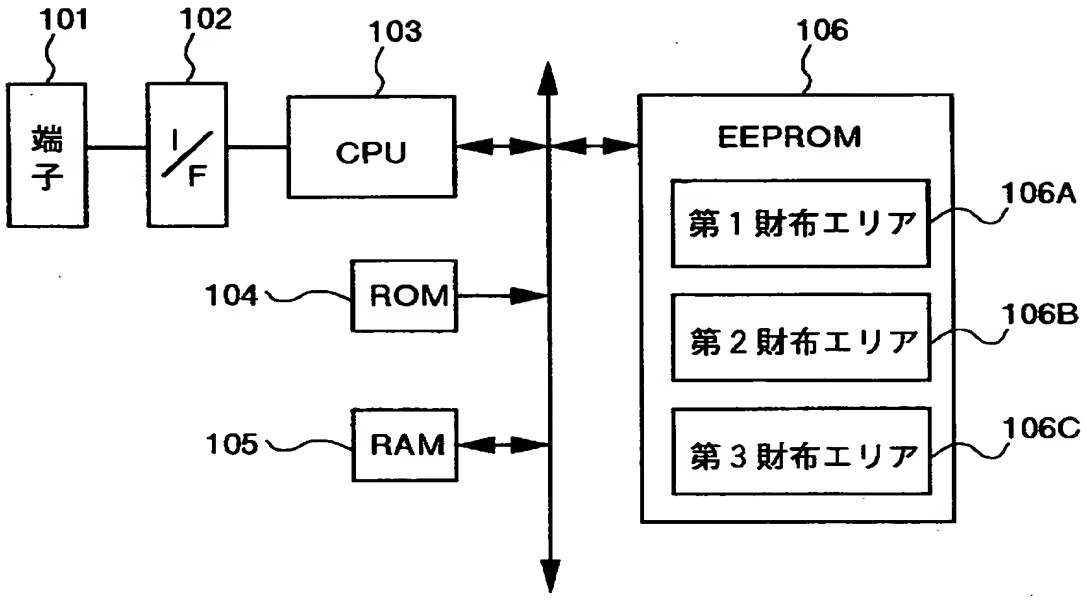
【図１】



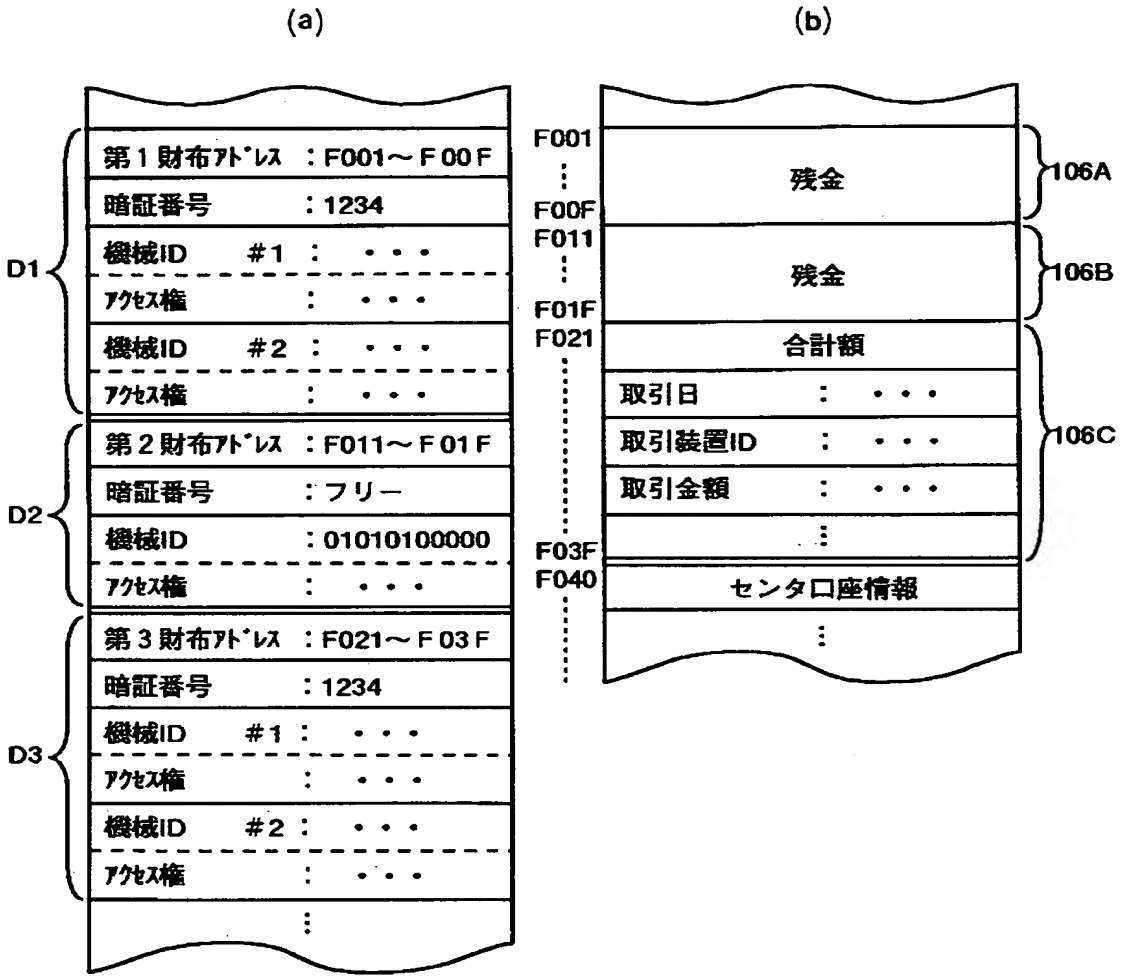
【図２】


11
要求領域識別部
12
復号化セキュリティ処理部
13
暗証番号処理部
14
照合処理部
15
アクセス権確認処理部
16
取引処理部

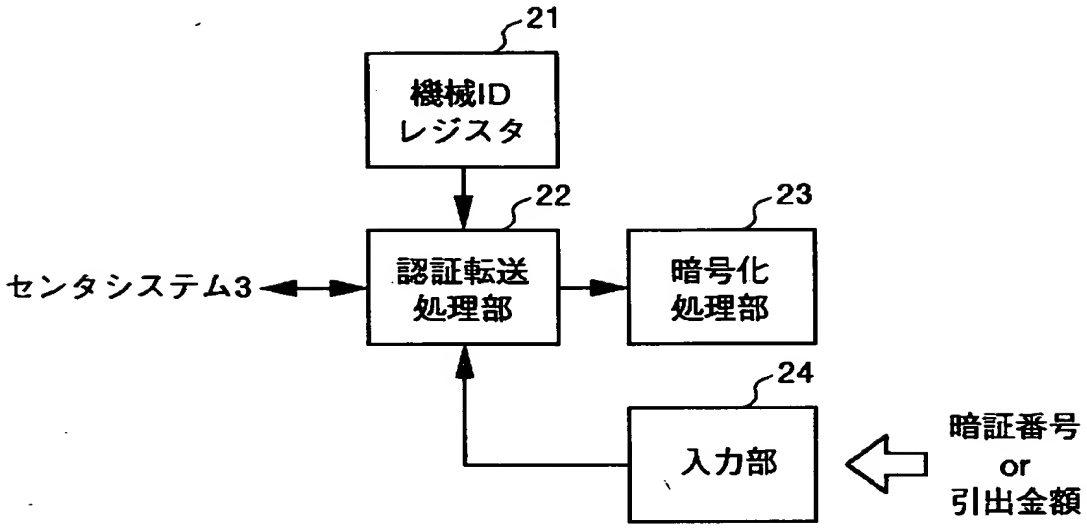
【図3】


101
102
103
106
端子
I/F
CPU
EEPROM
第1財布エリア
106A
104
ROM
第2財布エリア
106B
105
RAM
第3財布エリア
106C

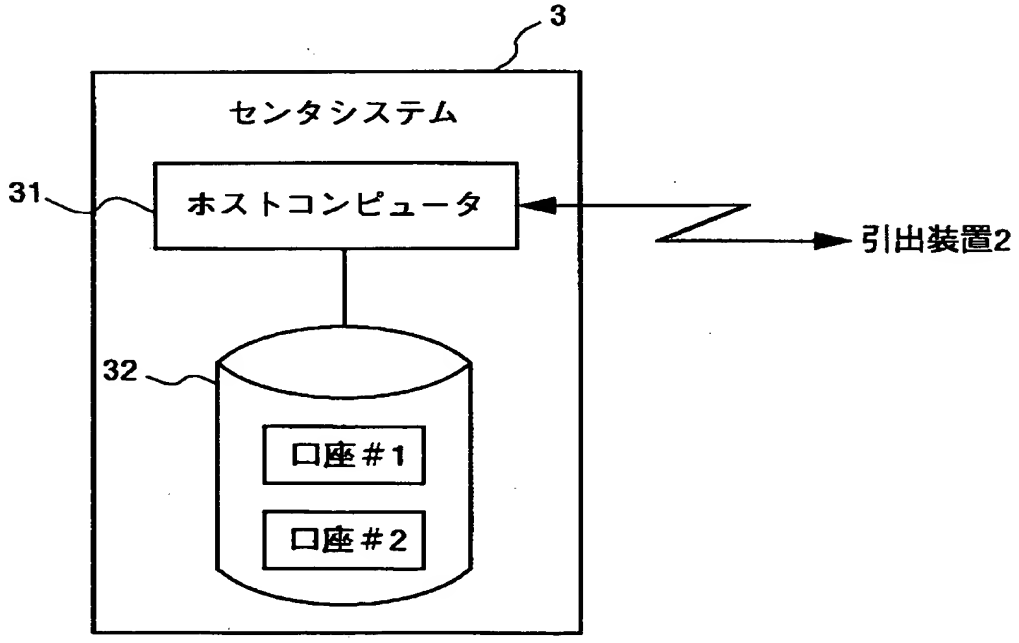
【図４】


(a)
(b)
D1
D2
D3
第１財布ｱﾄﾞﾚｽ　：F001～F00F
暗証番号　：1234
機械ID　#1　：・・・
ｱｸｾｽ権　：・・・
機械ID　#2　：・・・
ｱｸｾｽ権　：・・・
第２財布ｱﾄﾞﾚｽ　：F011～F01F
暗証番号　：フリー
機械ID　：01010100000
ｱｸｾｽ権　：・・・
第３財布ｱﾄﾞﾚｽ　：F021～F03F
暗証番号　：1234
機械ID　#1　：・・・
ｱｸｾｽ権　：・・・
機械ID　#2　：・・・
ｱｸｾｽ権　：・・・
F001
F00F
F011
F01F
F021
F03F
F040
残金
残金
合計額
取引日　：・・・
取引装置ID　：・・・
取引金額　：・・・
センタ口座情報
106A
106B
106C

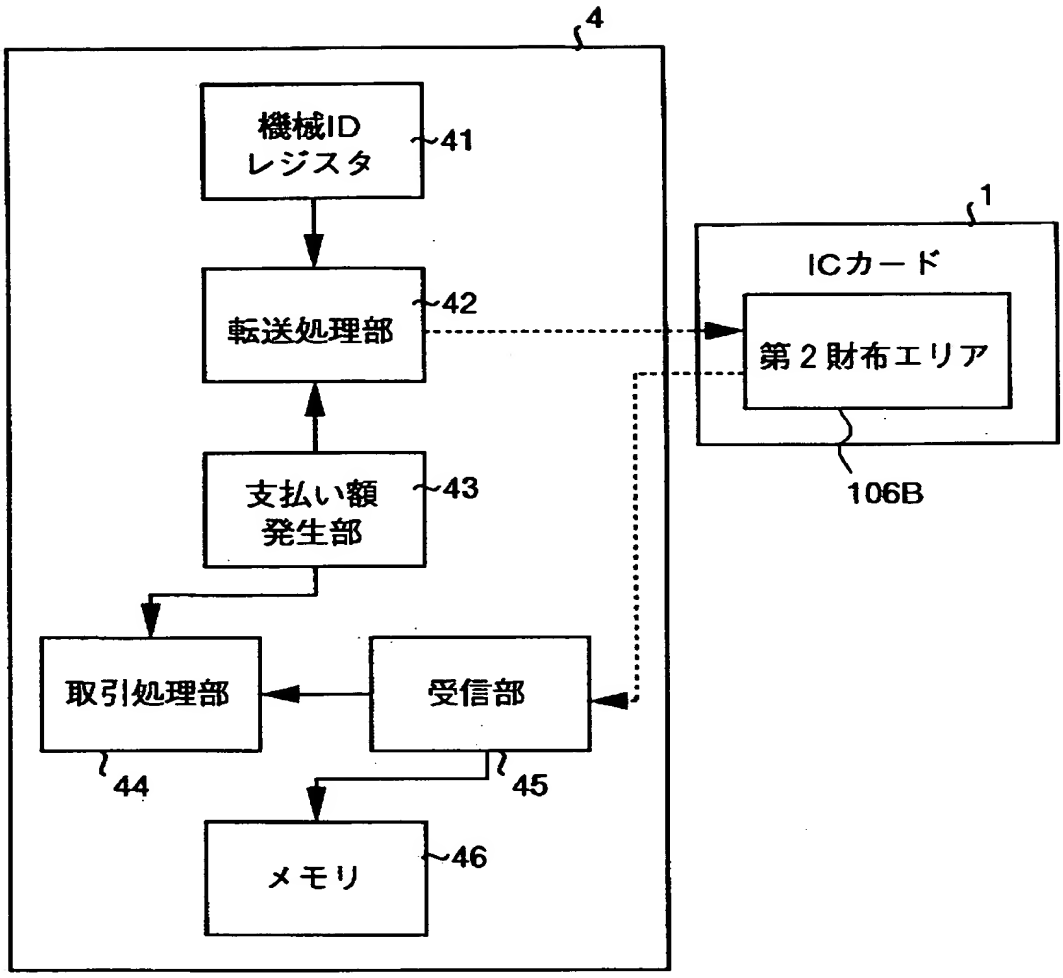
【図５】


21
機械ID
レジスタ
22
23
センタシステム3
認証転送
処理部
暗号化
処理部
24
入力部
暗証番号
or
引出金額

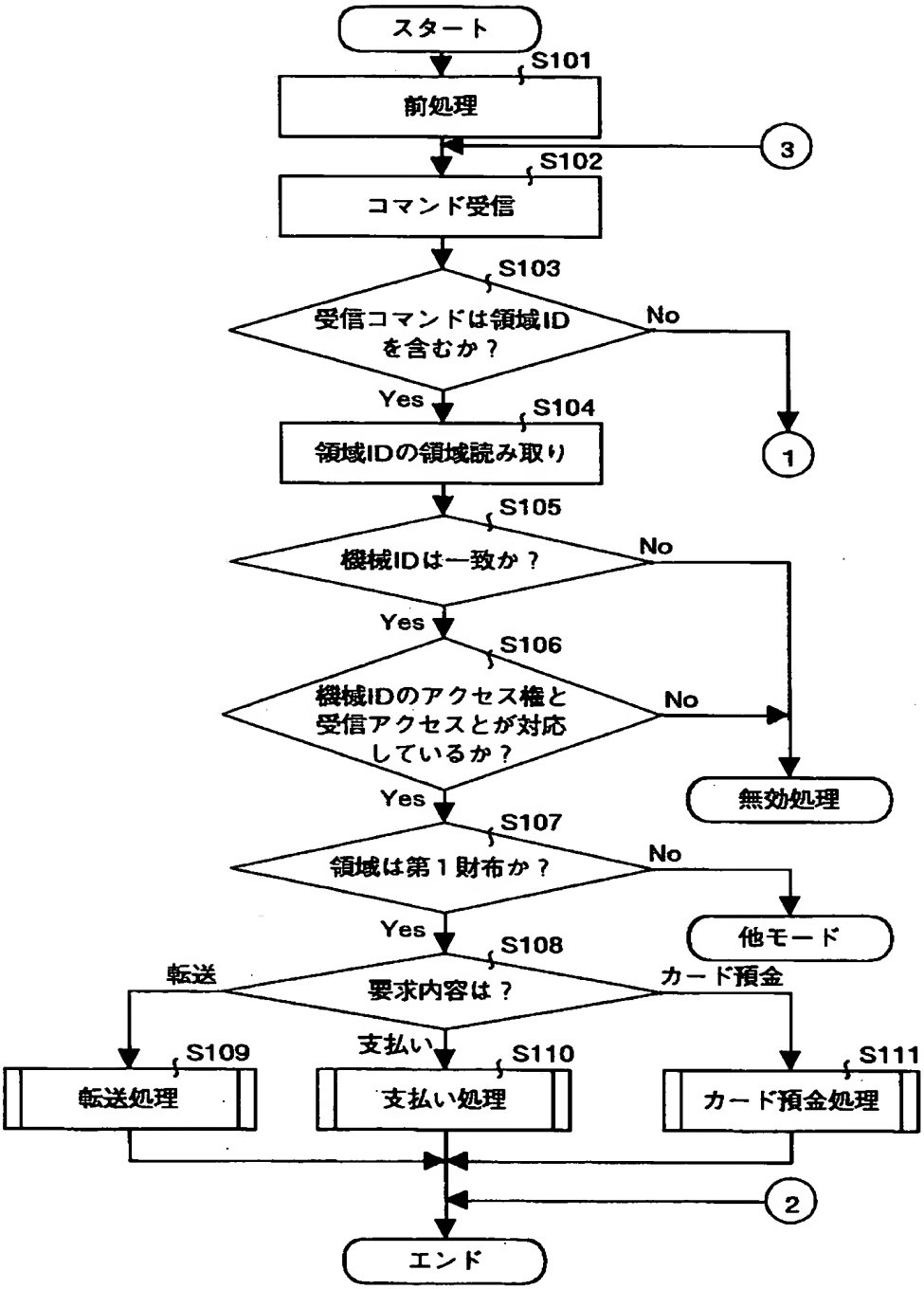
【図６】


3
センタシステム
31
ホストコンピュータ
引出装置2
32
口座＃1
口座＃2

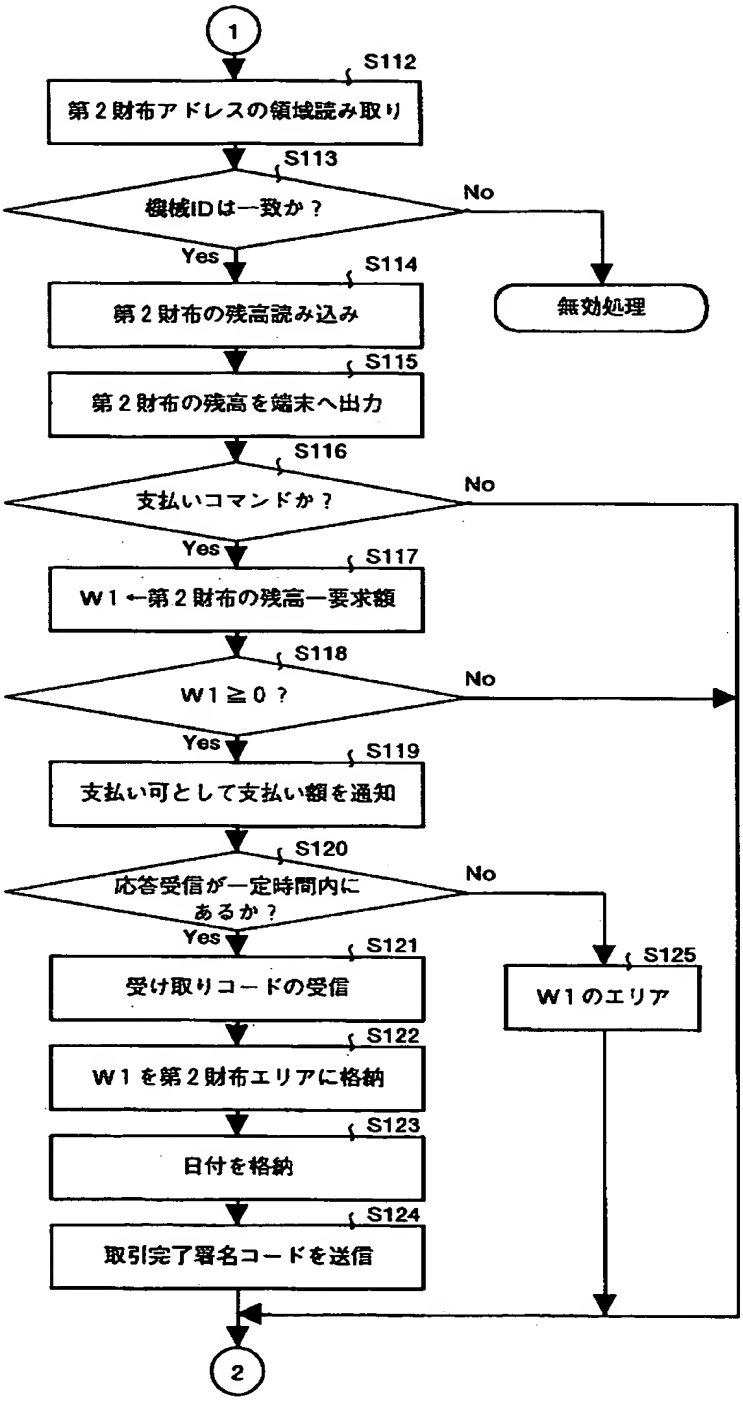
【図７】


4
機械ID
レジスタ
41
転送処理部
42
支払い額
発生部
43
取引処理部
44
受信部
45
メモリ
46
1
ICカード
第２財布エリア
106B

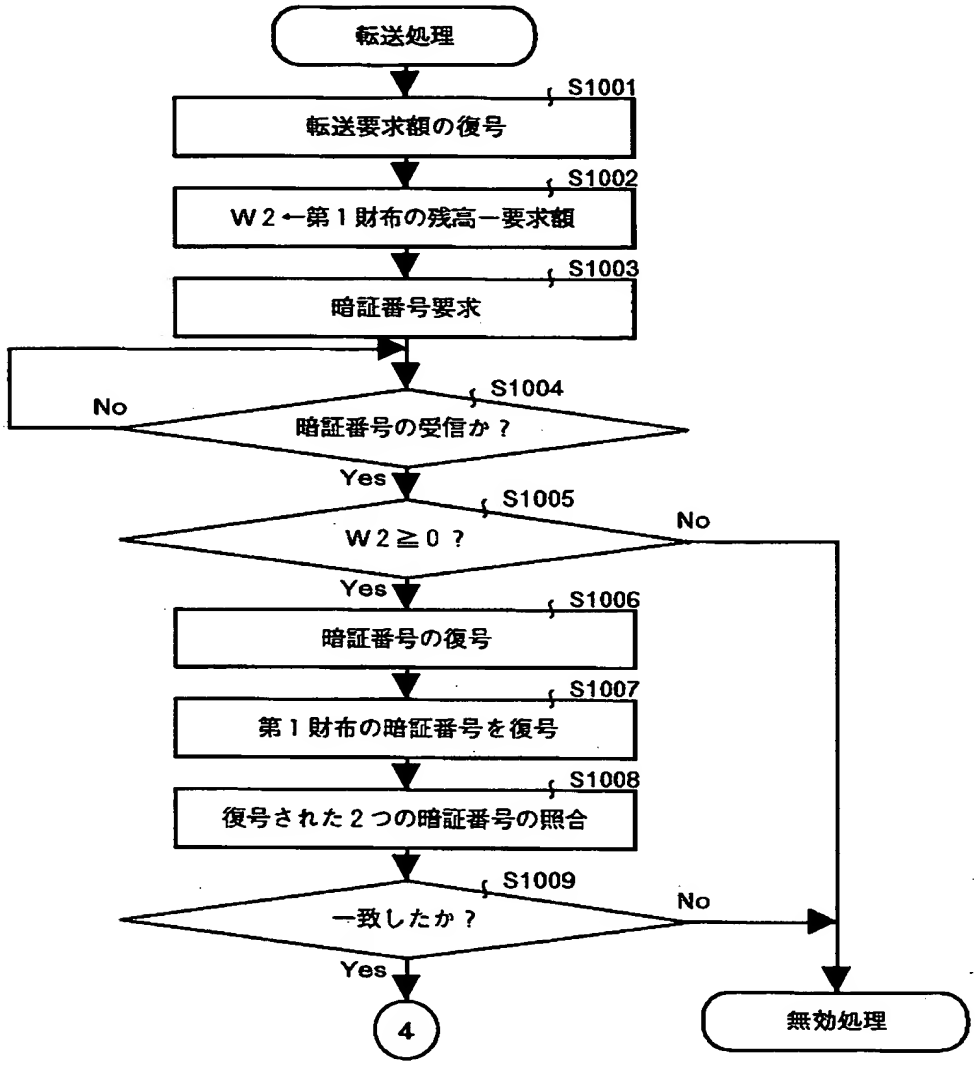
【図８】


スタート
S101
前処理
3
S102
コマンド受信
S103
受信コマンドは領域ID
を含むか？
No
Yes
S104
領域IDの領域読み取り
1
S105
機械IDは一致か？
No
Yes
S106
機械IDのアクセス権と
受信アクセスとが対応
しているか？
No
無効処理
Yes
S107
領域は第１財布か？
No
他モード
Yes
S108
要求内容は？
転送
支払い
カード預金
S109
転送処理
S110
支払い処理
S111
カード預金処理
2
エンド

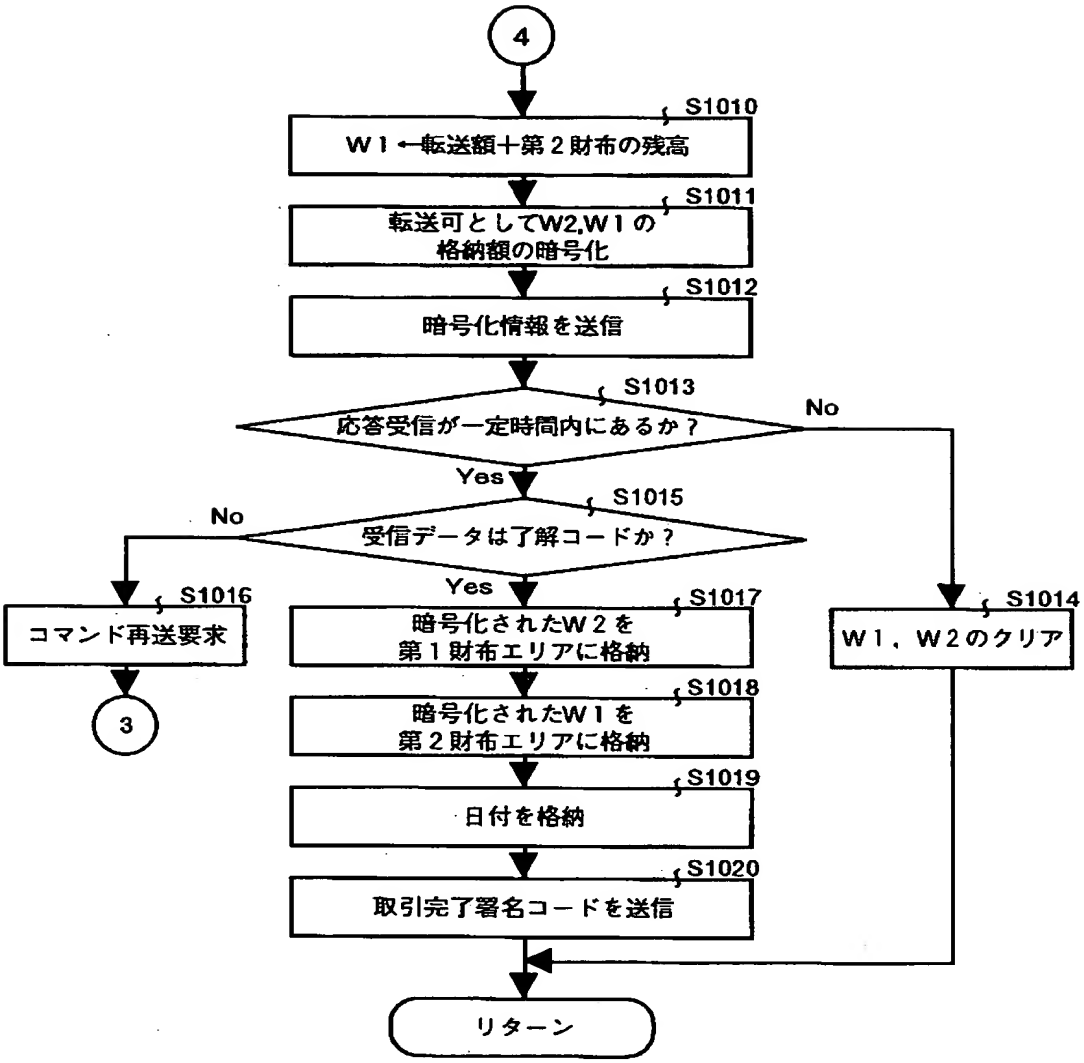
【図９】


1
S112
第２財布アドレスの領域読み取り
S113
機械IDは一致か？
No
Yes
S114
第２財布の残高読み込み
無効処理
S115
第２財布の残高を端末へ出力
S116
支払いコマンドか？
No
Yes
S117
W１←第２財布の残高－要求額
S118
W１≧０？
No
Yes
S119
支払い可として支払い額を通知
S120
応答受信が一定時間内にあるか？
No
Yes
S121
受け取りコードの受信
S125
W１のエリア
S122
W１を第２財布エリアに格納
S123
日付を格納
S124
取引完了署名コードを送信
2

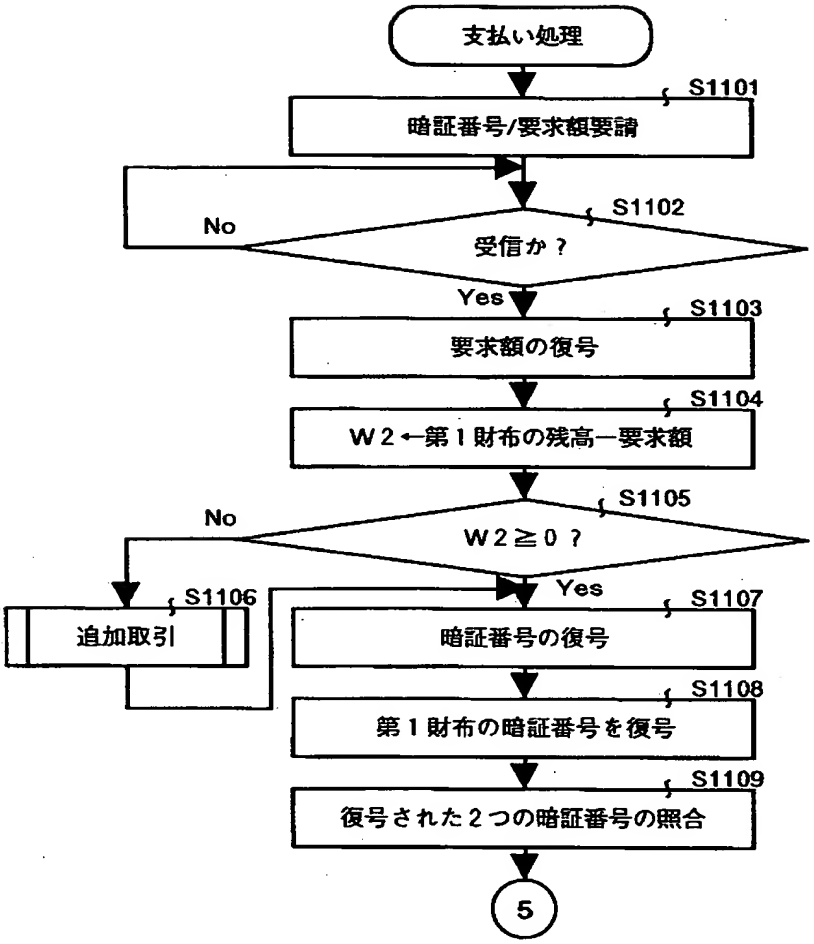
【図１０】


転送処理
S1001
転送要求額の復号
S1002
W２←第１財布の残高－要求額
S1003
暗証番号要求
S1004
No
暗証番号の受信か？
Yes
S1005
W２≧０？
No
Yes
S1006
暗証番号の復号
S1007
第１財布の暗証番号を復号
S1008
復号された２つの暗証番号の照合
S1009
一致したか？
No
Yes
4
無効処理

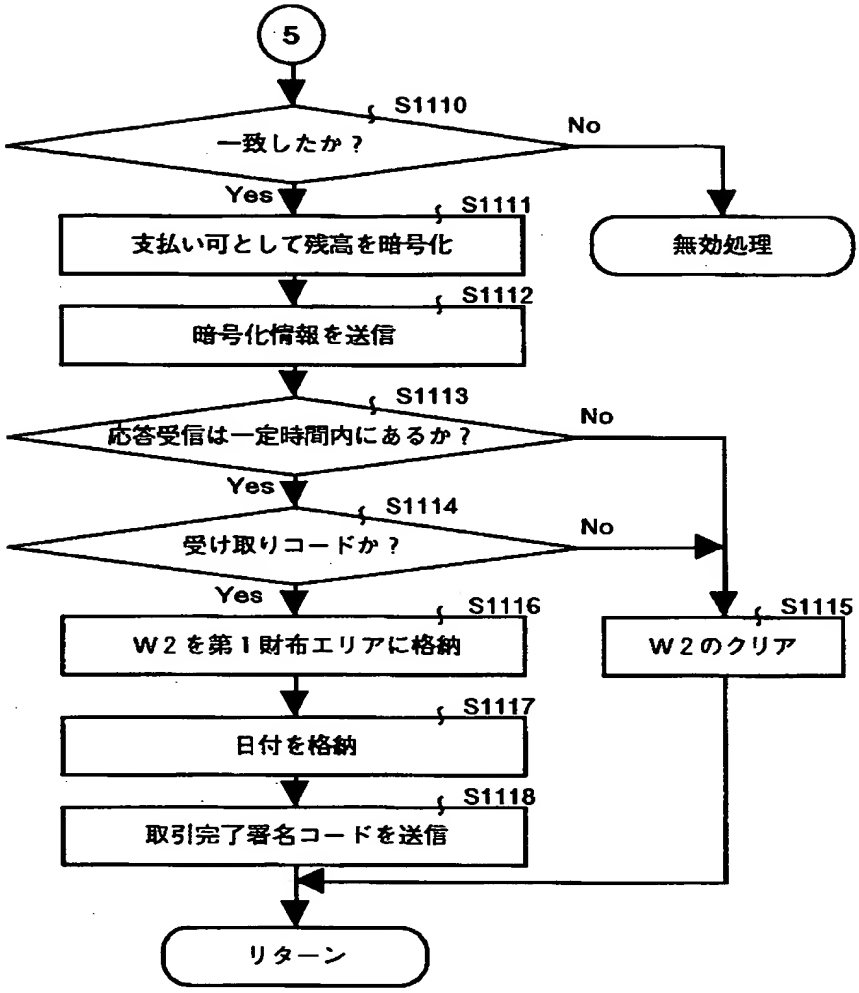
【図１１】


4
S1010
W１←転送額＋第２財布の残高
S1011
転送可としてW2,W１の
格納額の暗号化
S1012
暗号化情報を送信
S1013
応答受信が一定時間内にあるか？
No
Yes
S1015
受信データは了解コードか？
No
Yes
S1016
コマンド再送要求
3
S1017
暗号化されたW２を
第１財布エリアに格納
S1018
暗号化されたW１を
第２財布エリアに格納
S1019
日付を格納
S1020
取引完了署名コードを送信
S1014
W１，W２のクリア
リターン

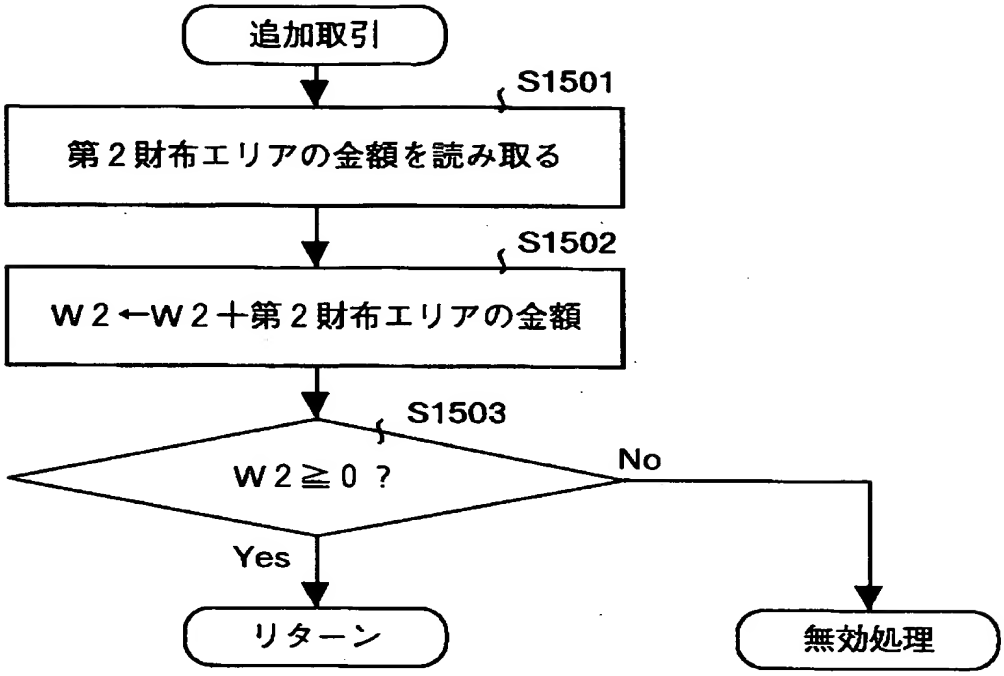
【図１２】


支払い処理
S1101
暗証番号/要求額要請
S1102
No
受信か？
Yes
S1103
要求額の復号
S1104
W２←第１財布の残高−要求額
S1105
No
W２≧０？
Yes
S1106
追加取引
S1107
暗証番号の復号
S1108
第１財布の暗証番号を復号
S1109
復号された２つの暗証番号の照合
5

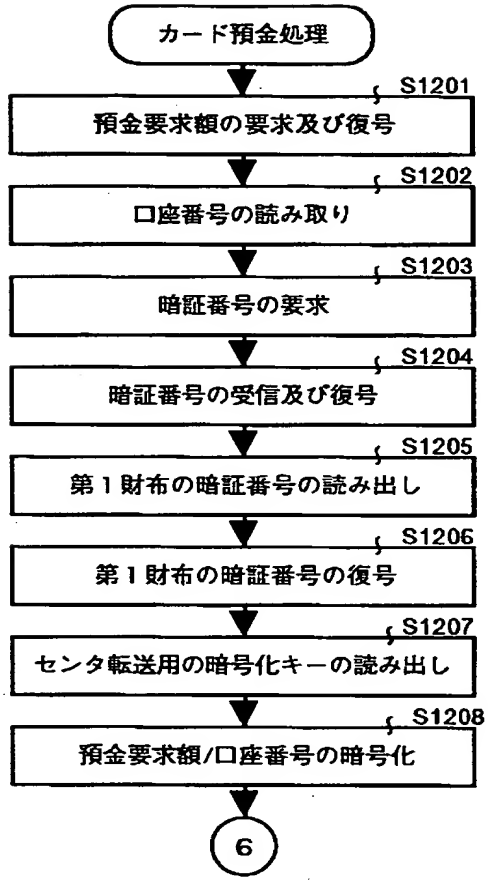
【図１３】


5
S1110
一致したか？
No
Yes
S1111
支払い可として残高を暗号化
無効処理
S1112
暗号化情報を送信
S1113
応答受信は一定時間内にあるか？
No
Yes
S1114
受け取りコードか？
No
Yes
S1116
W２を第１財布エリアに格納
S1115
W２のクリア
S1117
日付を格納
S1118
取引完了署名コードを送信
リターン

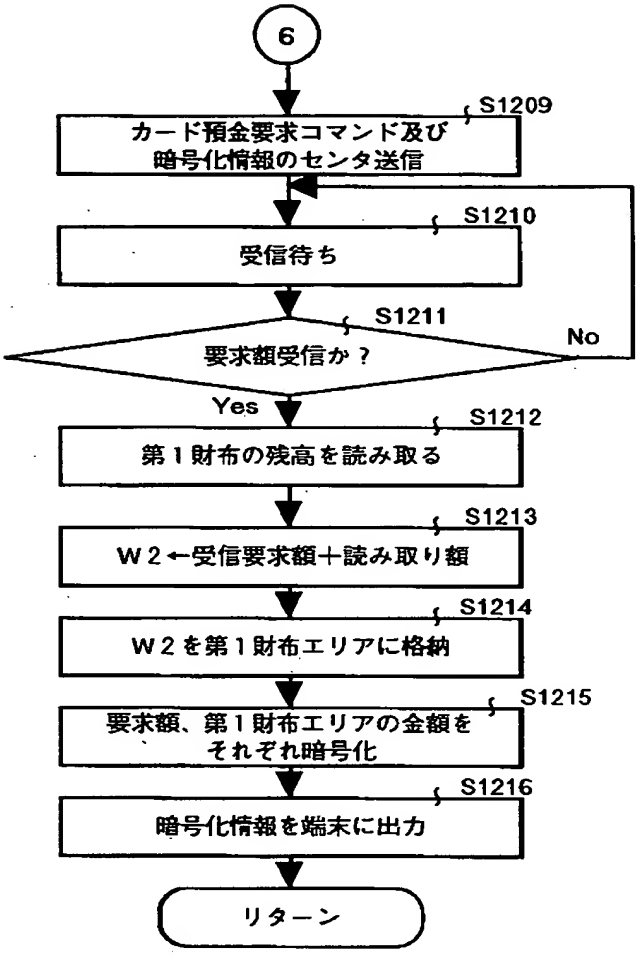
【図１４】


追加取引
S1501
第２財布エリアの金額を読み取る
S1502
Ｗ２←Ｗ２＋第２財布エリアの金額
S1503
Ｗ２≧０？
No
Yes
リターン
無効処理

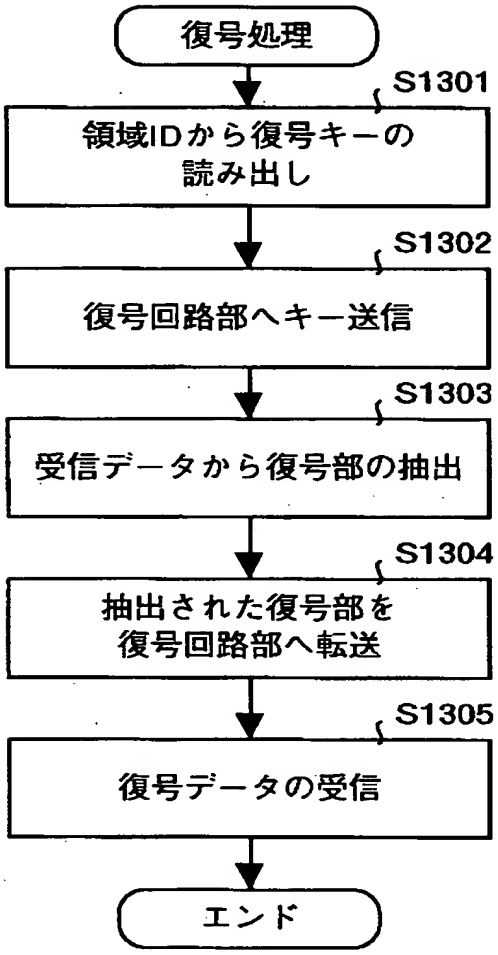
【図１５】


カード預金処理
S1201
預金要求額の要求及び復号
S1202
口座番号の読み取り
S1203
暗証番号の要求
S1204
暗証番号の受信及び復号
S1205
第１財布の暗証番号の読み出し
S1206
第１財布の暗証番号の復号
S1207
センタ転送用の暗号化キーの読み出し
S1208
預金要求額/口座番号の暗号化
6

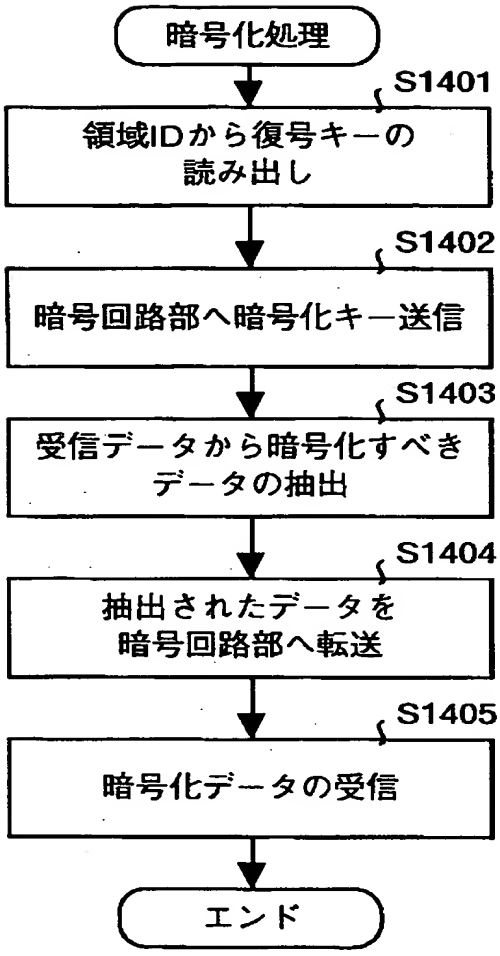
【図１６】


6
S1209
カード預金要求コマンド及び
暗号化情報のセンタ送信
S1210
受信待ち
S1211
要求額受信か？
No
Yes
S1212
第１財布の残高を読み取る
S1213
Ｗ２←受信要求額＋読み取り額
S1214
Ｗ２を第１財布エリアに格納
S1215
要求額、第１財布エリアの金額を
それぞれ暗号化
S1216
暗号化情報を端末に出力
リターン

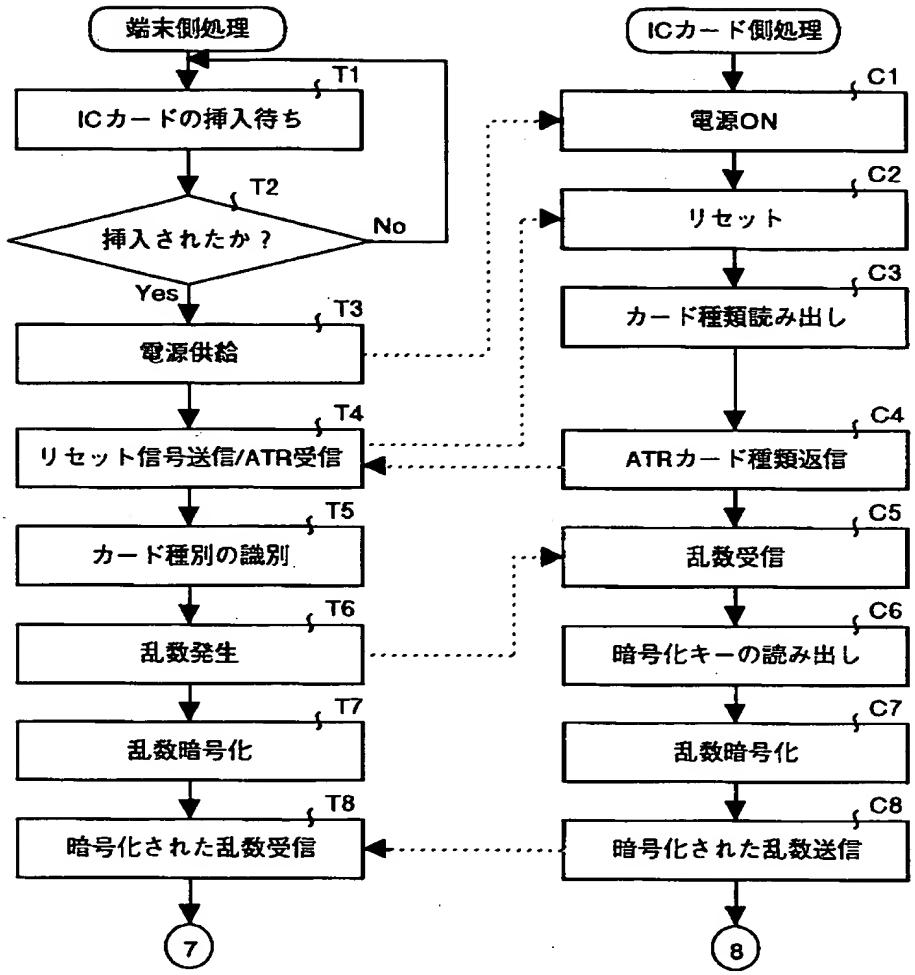
【図１７】


復号処理
S1301
領域IDから復号キーの
読み出し
S1302
復号回路部へキー送信
S1303
受信データから復号部の抽出
S1304
抽出された復号部を
復号回路部へ転送
S1305
復号データの受信
エンド

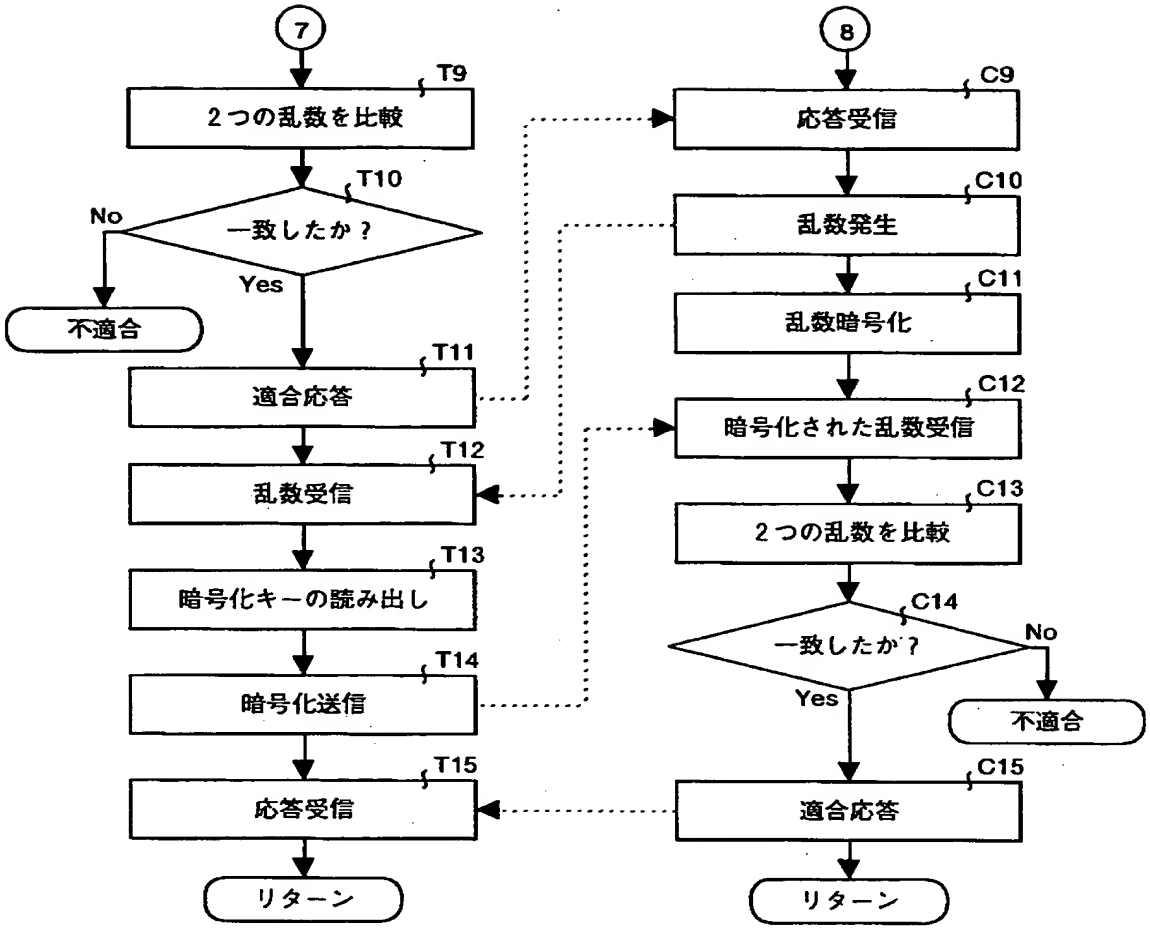
【図１８】


暗号化処理
S1401
領域IDから復号キーの
読み出し
S1402
暗号回路部へ暗号化キー送信
S1403
受信データから暗号化すべき
データの抽出
S1404
抽出されたデータを
暗号回路部へ転送
S1405
暗号化データの受信
エンド

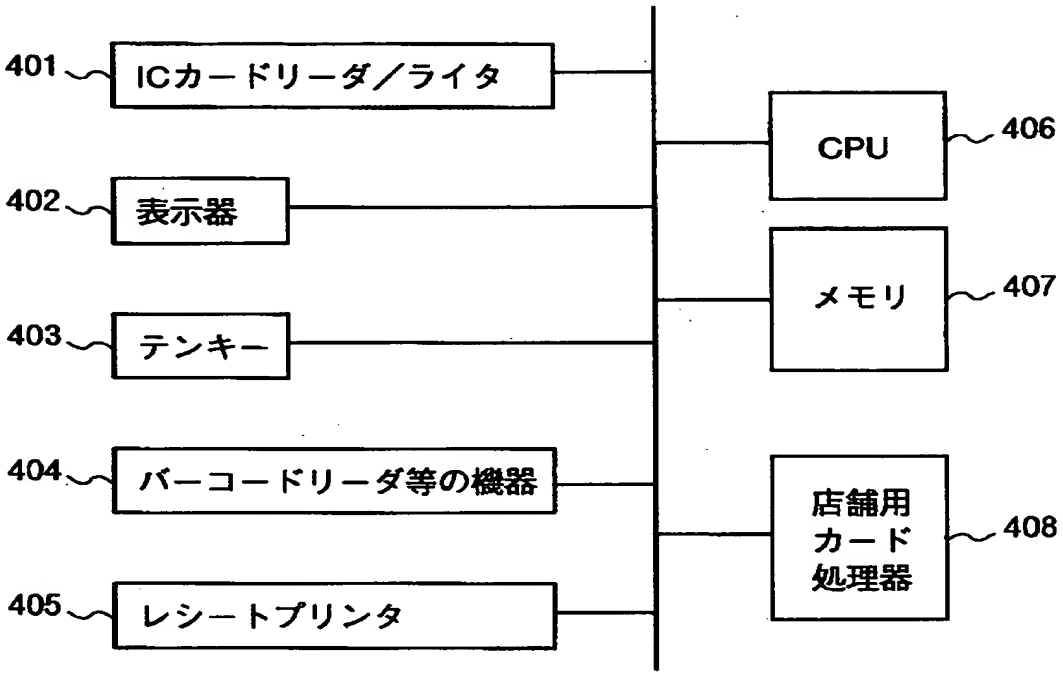
【図１９】


端末側処理
ICカードの挿入待ち
T1
挿入されたか？
T2
No
Yes
電源供給
T3
リセット信号送信/ATR受信
T4
カード種別の識別
T5
乱数発生
T6
乱数暗号化
T7
暗号化された乱数受信
T8
7
ICカード側処理
電源ON
C1
リセット
C2
カード種類読み出し
C3
ATRカード種類返信
C4
乱数受信
C5
暗号化キーの読み出し
C6
乱数暗号化
C7
暗号化された乱数送信
C8
8

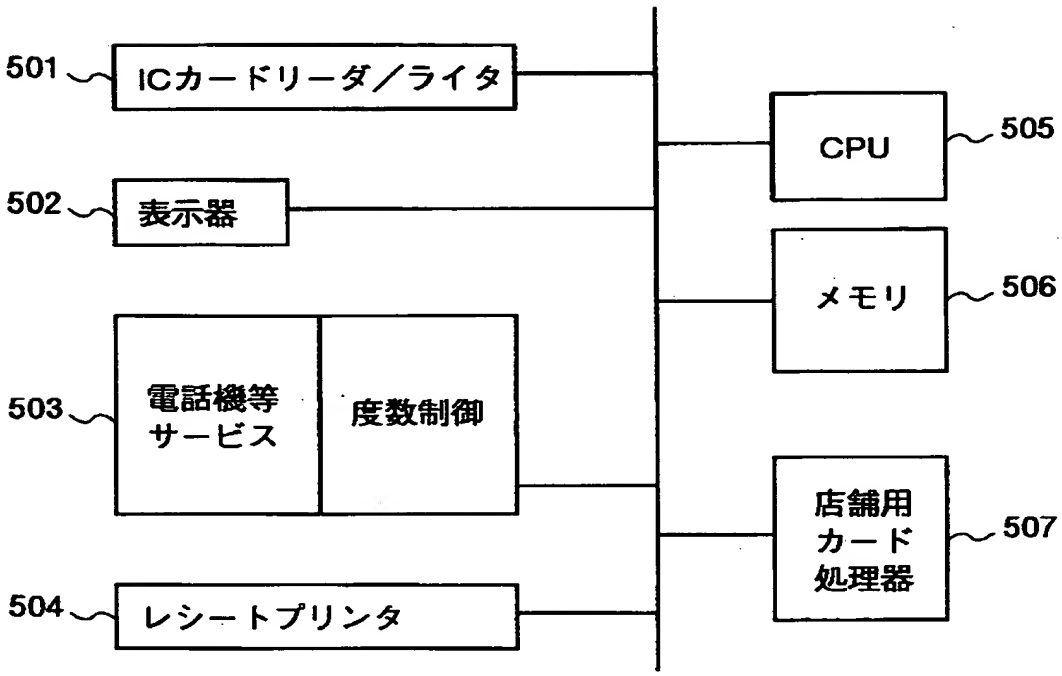
【図２０】


7
T9
２つの乱数を比較
T10
No
一致したか？
Yes
不適合
T11
適合応答
T12
乱数受信
T13
暗号化キーの読み出し
T14
暗号化送信
T15
応答受信
リターン
8
C9
応答受信
C10
乱数発生
C11
乱数暗号化
C12
暗号化された乱数受信
C13
２つの乱数を比較
C14
一致したか？
No
Yes
不適合
C15
適合応答
リターン

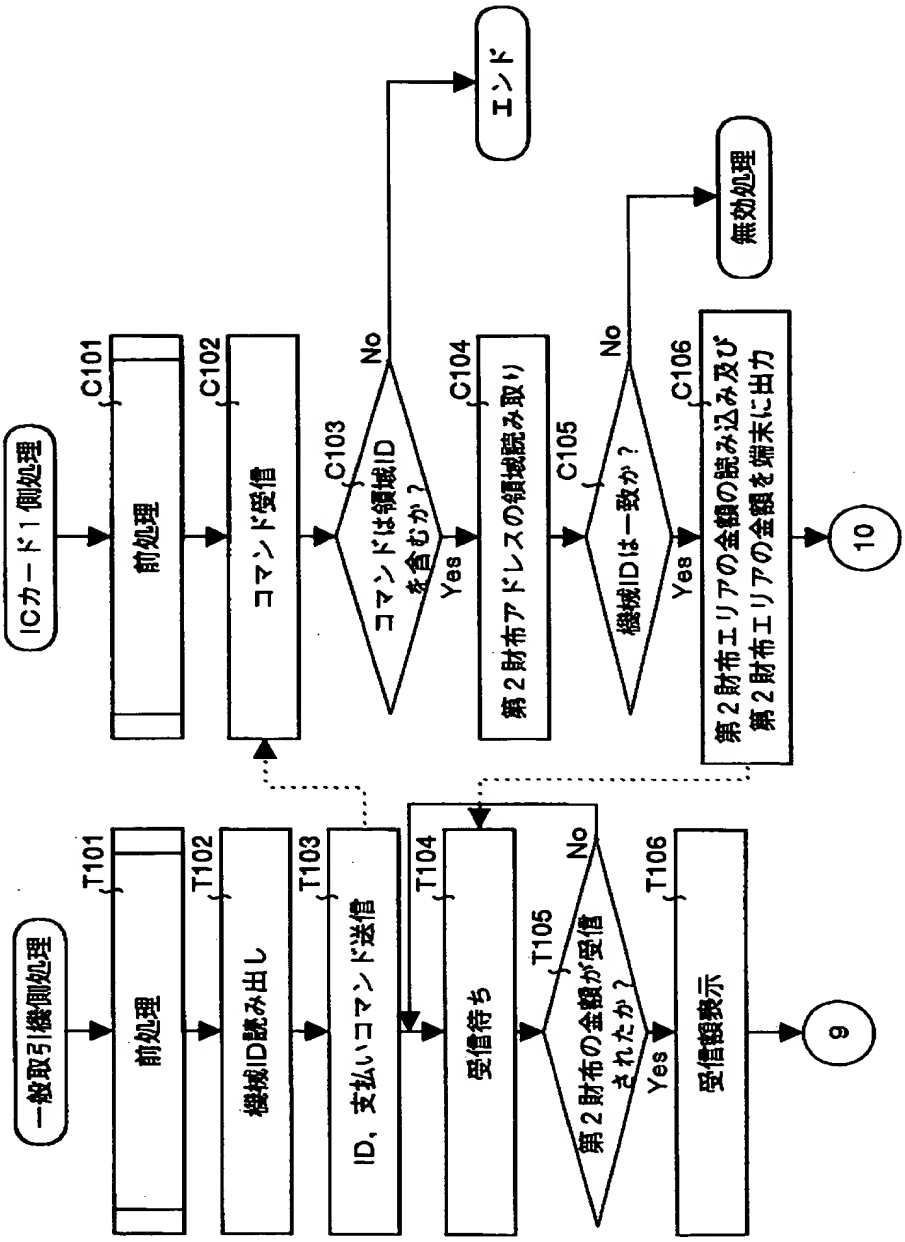
【図２１】


401
ICカードリーダ／ライタ
402
表示器
403
テンキー
404
バーコードリーダ等の機器
405
レシートプリンタ
CPU
406
メモリ
407
店舗用
カード
処理器
408

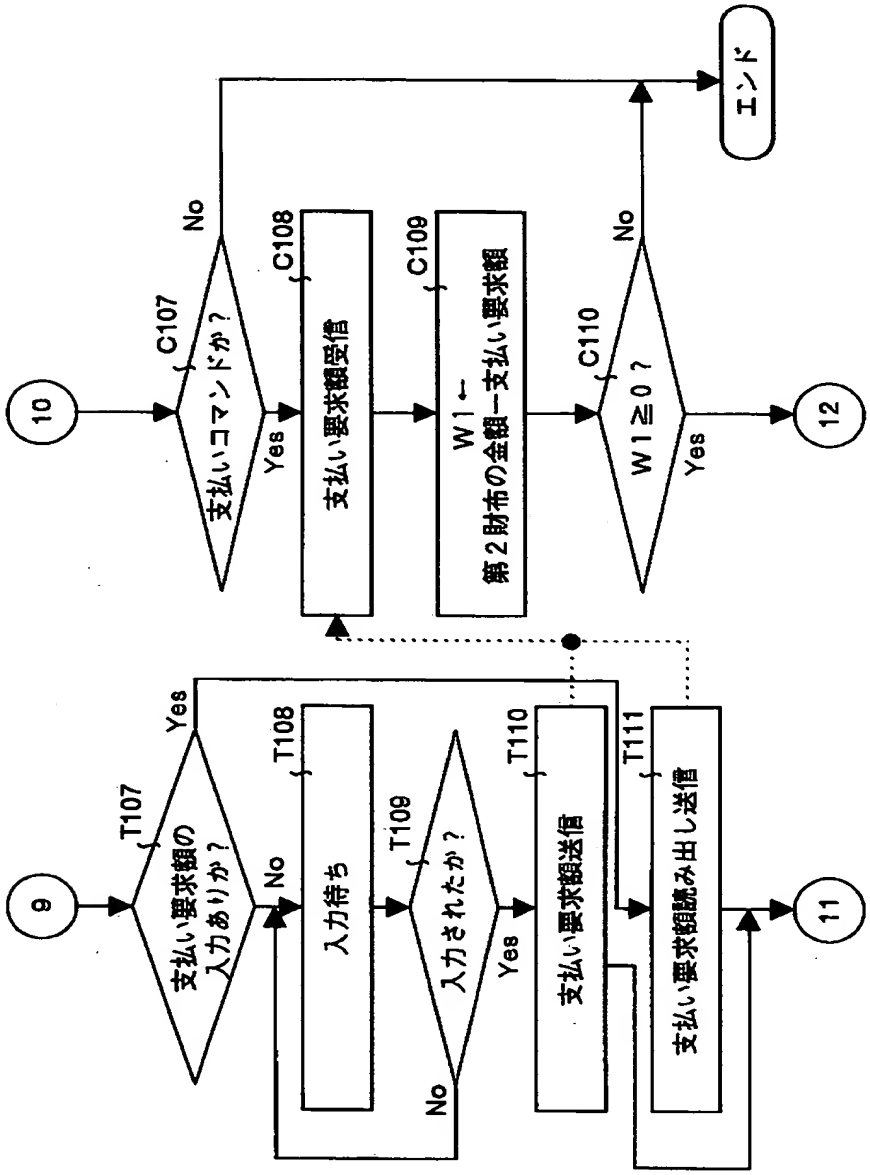
【図２２】


501
ICカードリーダ／ライタ
502
表示器
503
電話機等
サービス
度数制御
504
レシートプリンタ
CPU
505
メモリ
506
店舗用
カード
処理器
507

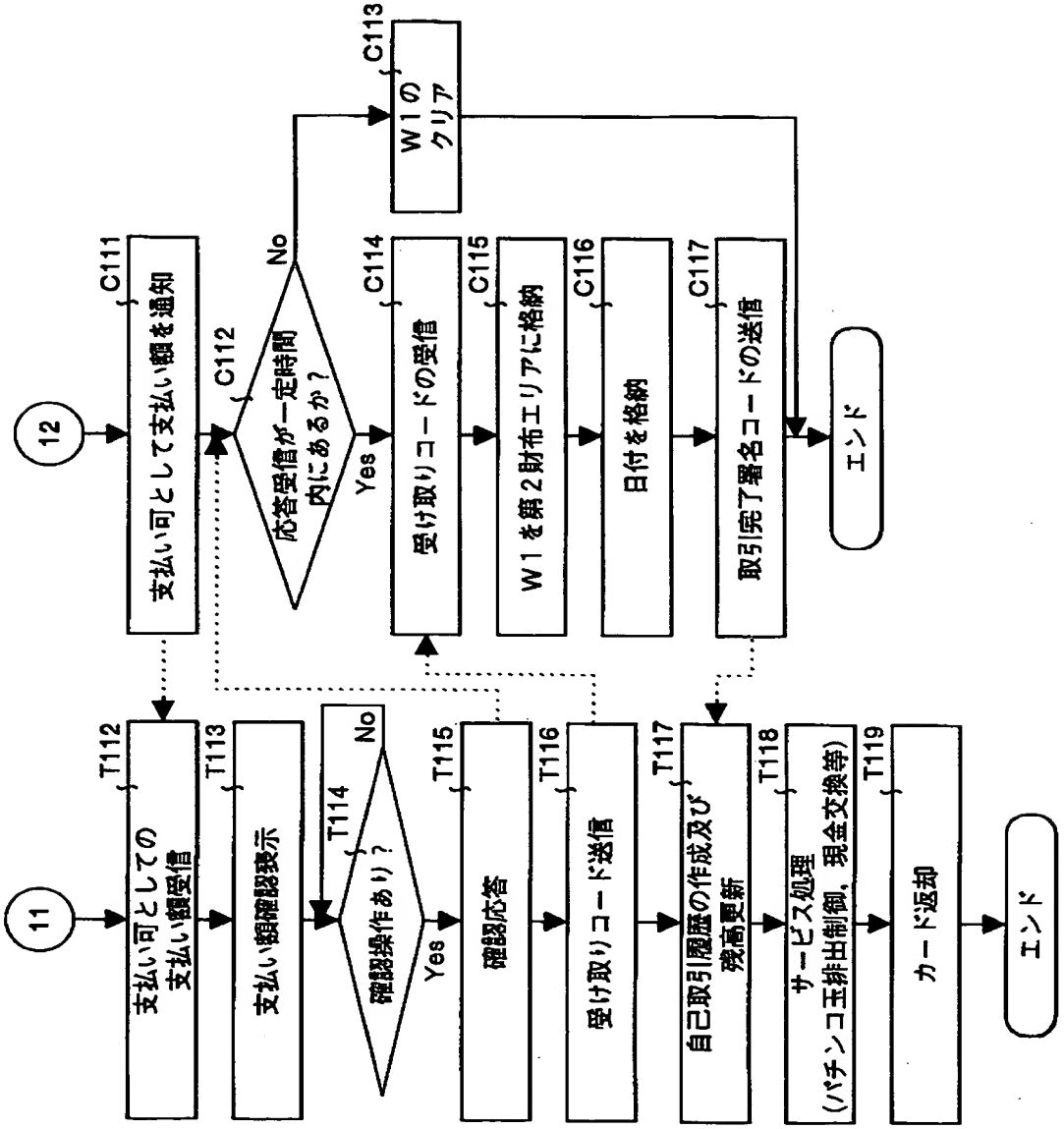
【図２３】


ICカード1側処理
前処理
C101
コマンド受信
C102
コマンドは領域IDを含むか？
C103
No
Yes
エンド
第2財布アドレスの領域読み取り
C104
機械IDは一致か？
C105
No
Yes
無効処理
第2財布エリアの金額の読み込み及び第2財布エリアの金額を端末に出力
C106
10
一般取引機側処理
前処理
T101
機械ID読み出し
T102
ID、支払いコマンド送信
T103
受信待ち
T104
第2財布の金額が受信されたか？
T105
No
Yes
受信額表示
T106
9

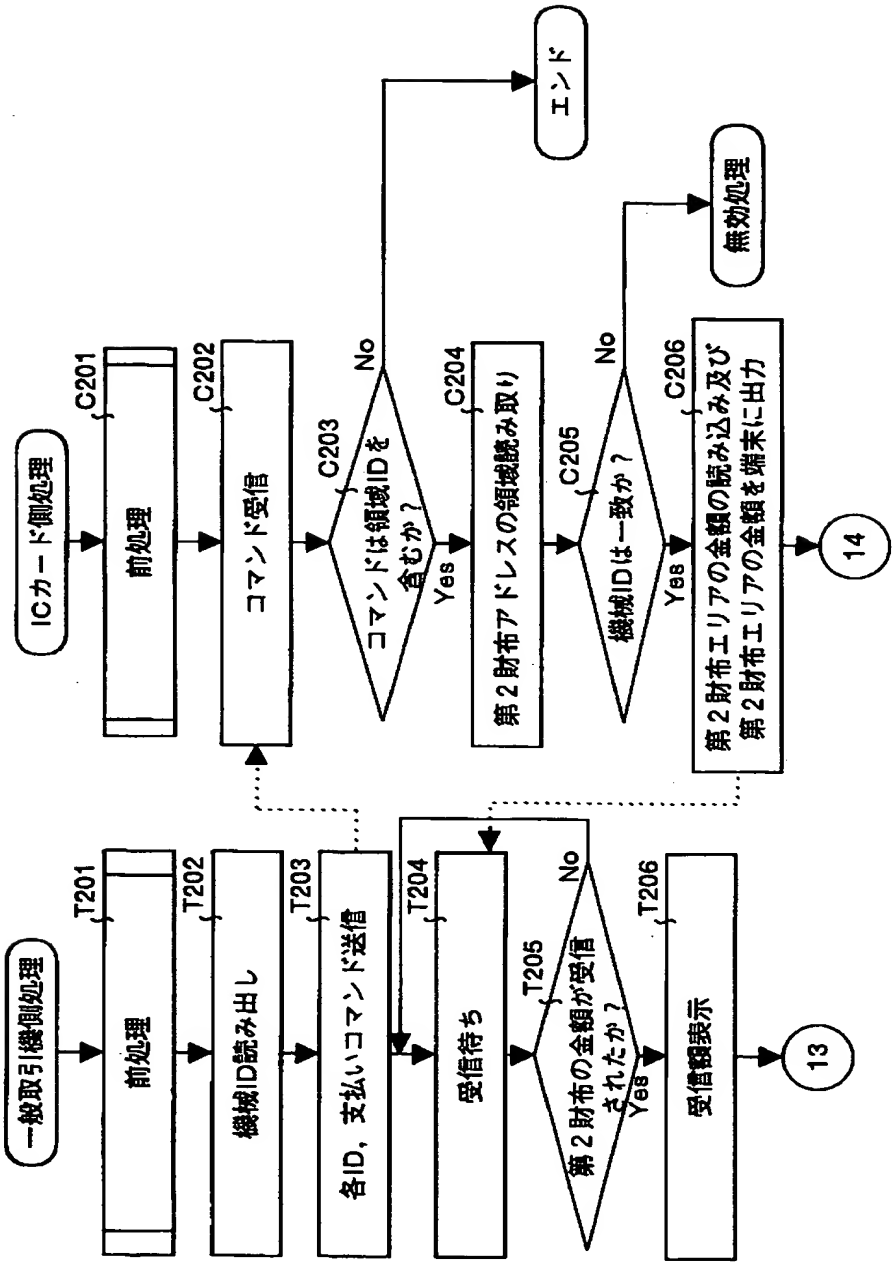
【図２４】


エンド
No
C107
支払いコマンドか？
Yes
C108
支払い要求額受信
C109
W1←
第２財布の金額－支払い要求額
C110
No
W1≧0？
Yes
10
12
Yes
T107
支払い要求額の
入力ありか？
No
T108
入力待ち
T109
入力されたか？
No
Yes
T110
支払い要求額送信
T111
支払い要求額読み出し送信
9
11

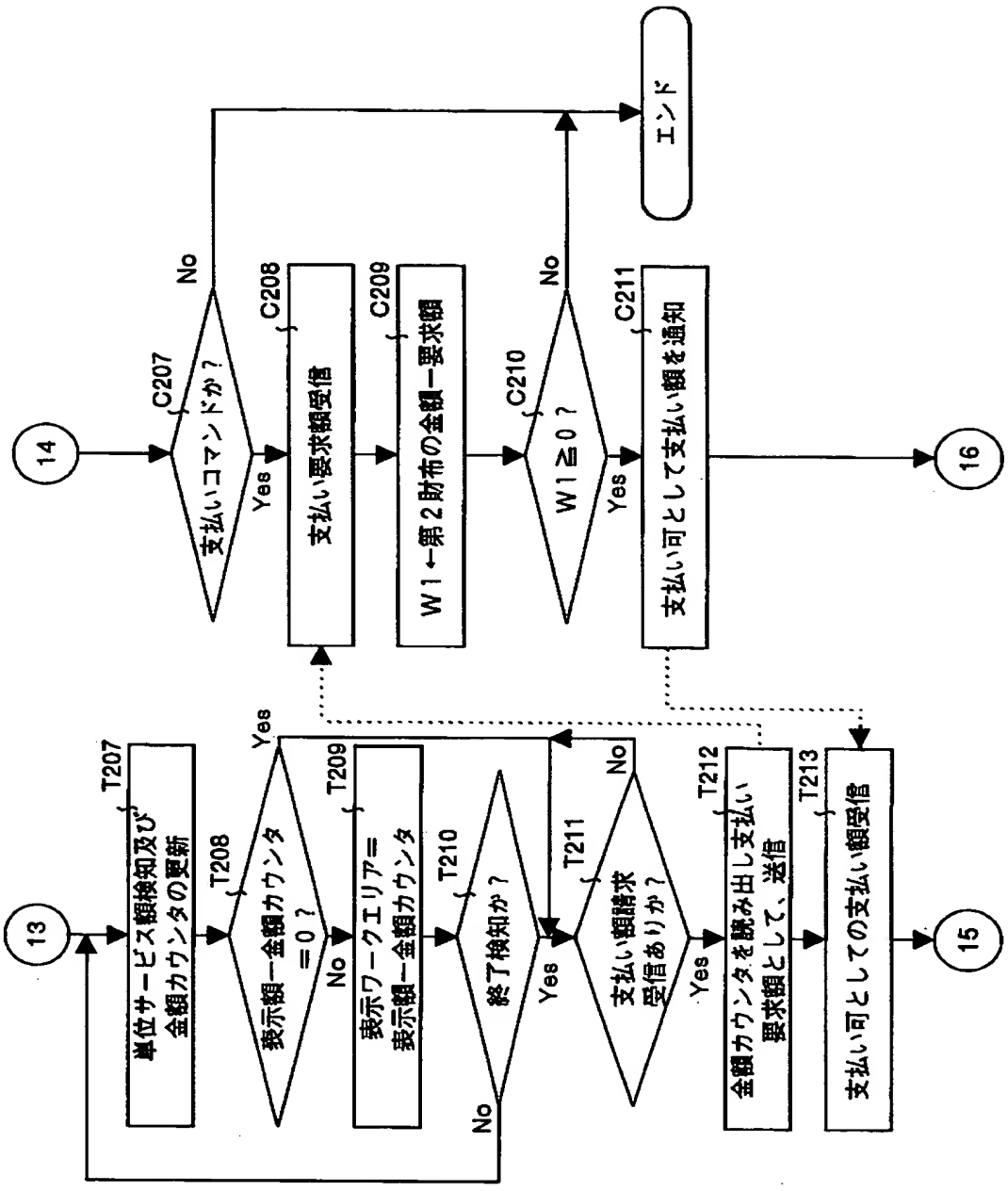
【図２５】


11
12
T112
支払い可としての
支払い額受信
T113
支払い額確認表示
T114
確認操作あり？
No
Yes
T115
確認応答
T116
受け取りコード送信
T117
自己取引履歴の作成及び
残高更新
T118
サービス処理
(パチンコ玉排出制御，現金交換等)
T119
カード返却
エンド
C111
支払い可として支払い額を通知
C112
応答受信が一定時間
内にあるか？
No
Yes
C113
W1の
クリア
C114
受け取りコードの受信
C115
W1を第2財布エリアに格納
C116
日付を格納
C117
取引完了署名コードの送信
エンド

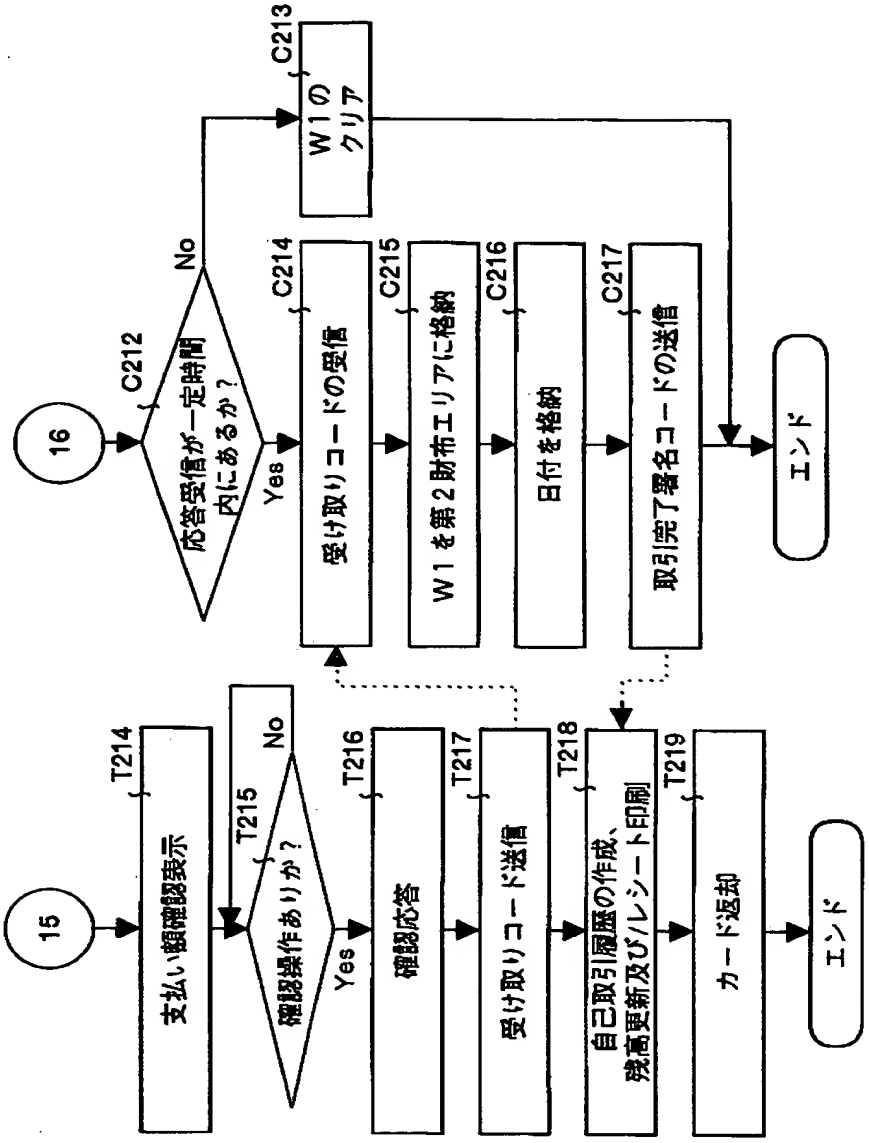
【図２６】


一般取引機側処理
T201
前処理
T202
機械ID読み出し
T203
各ID，支払いコマンド送信
T204
受信待ち
T205
第２財布の金額が受信されたか？
No
Yes
T206
受信額表示
13
ICカード側処理
C201
前処理
C202
コマンド受信
C203
コマンドは領域IDを含むか？
No
Yes
エンド
C204
第２財布アドレスの領域読み取り
C205
機械IDは一致か？
No
Yes
無効処理
C206
第２財布エリアの金額の読み込み及び第２財布エリアの金額を端末に出力
14

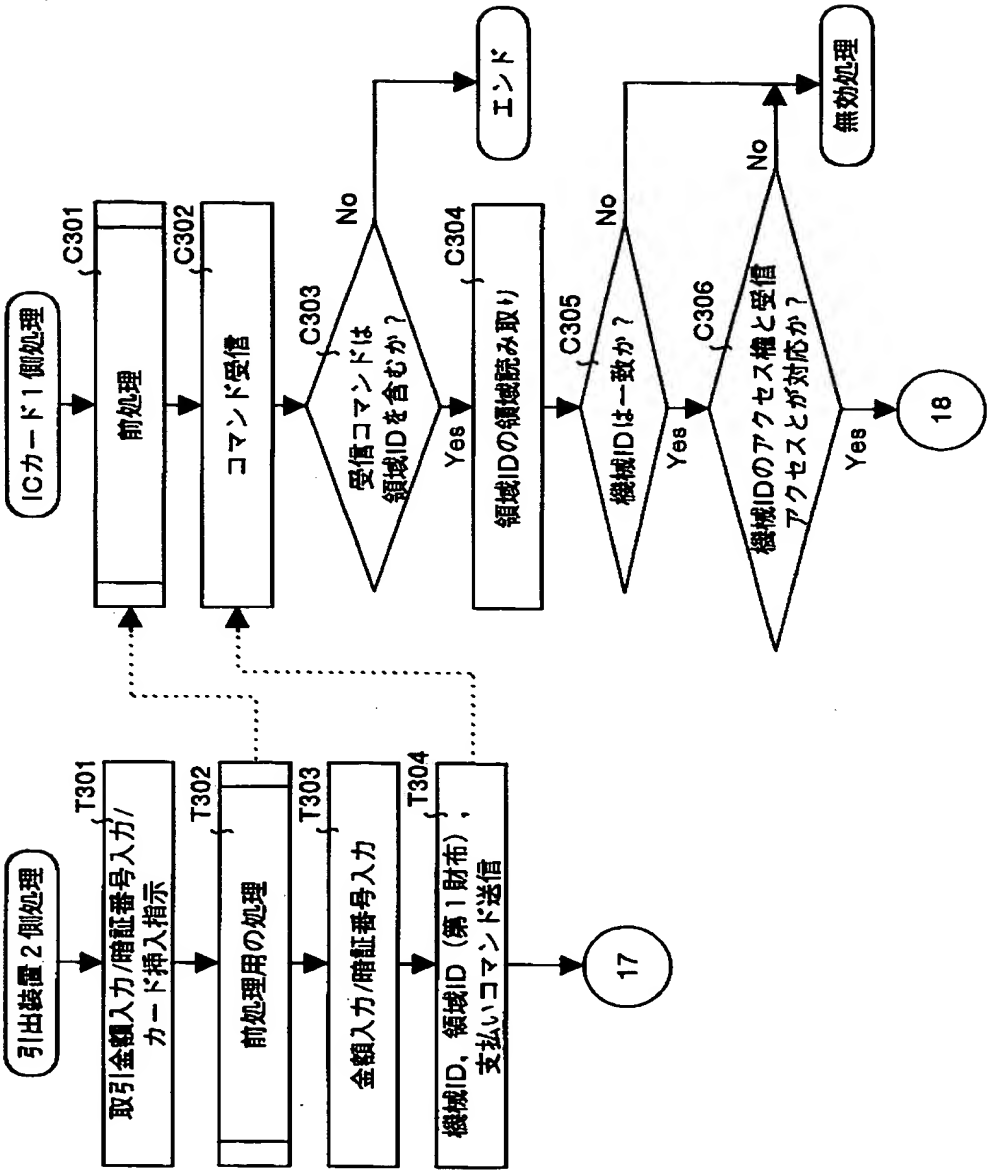
【図２７】


13
14
15
16
T207
単位サービス額検知及び
金額カウンタの更新
T208
表示額－金額カウンタ
＝０？
Yes
No
T209
表示ワークエリア＝
表示額－金額カウンタ
T210
終了検知か？
Yes
No
T211
支払い額請求
受信ありか？
No
Yes
T212
金額カウンタを読み出し支払い
要求額として、送信
T213
支払い可としての支払い額受信
C207
支払いコマンドか？
No
Yes
C208
支払い要求額受信
C209
W１←第２財布の金額－要求額
C210
W１≧０？
No
Yes
C211
支払い可として支払い額を通知
エンド

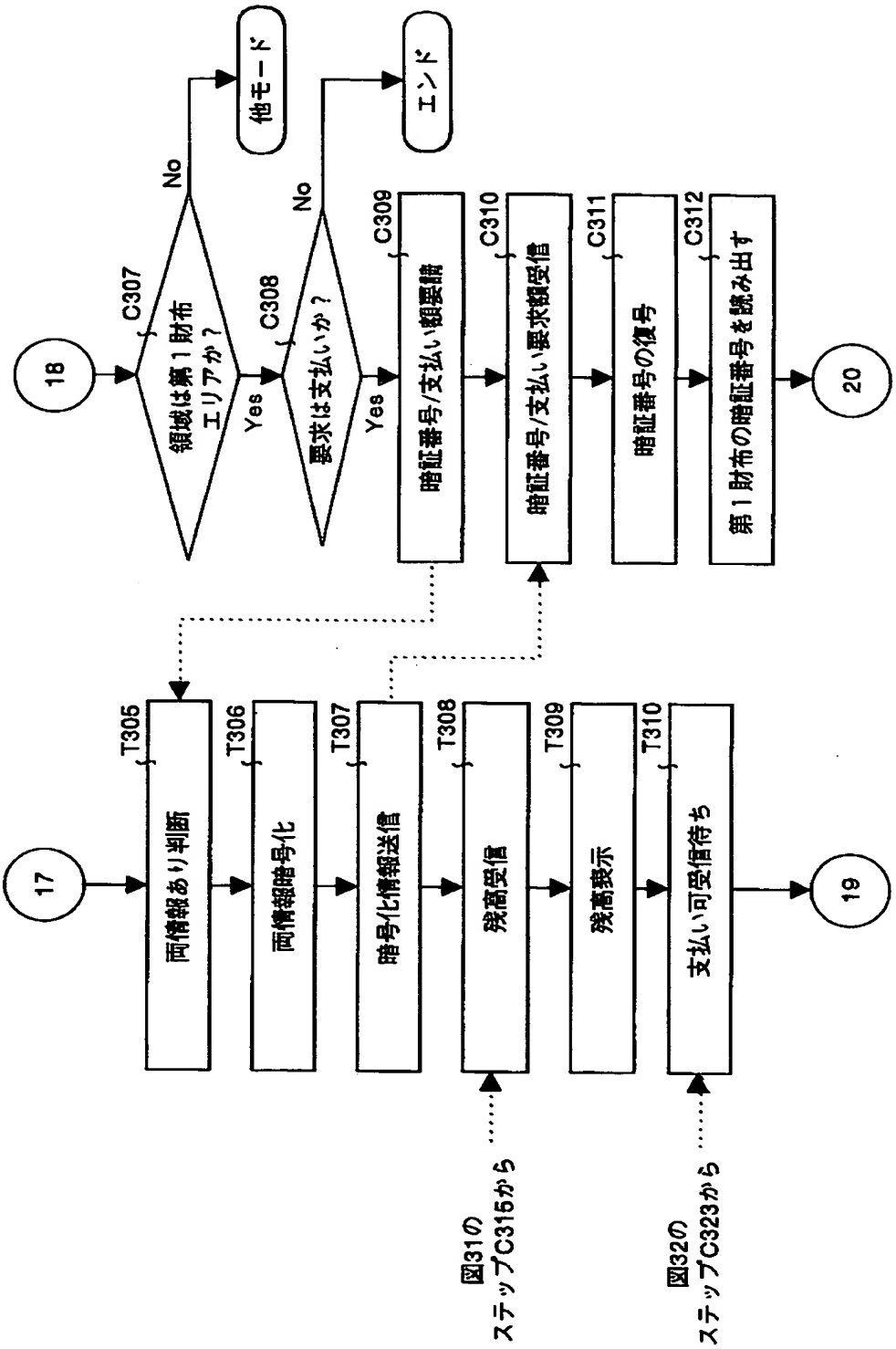
【図２８】


15
T214
支払い額確認表示
T215
確認操作ありか？
No
Yes
T216
確認応答
T217
受け取りコード送信
T218
自己取引履歴の作成、
残高更新及び/レシート印刷
T219
カード返却
エンド
16
C212
応答受信が一定時間
内にあるか？
No
Yes
C213
W1の
クリア
C214
受け取りコードの受信
C215
W1を第2財布エリアに格納
C216
日付を格納
C217
取引完了署名コードの送信
エンド

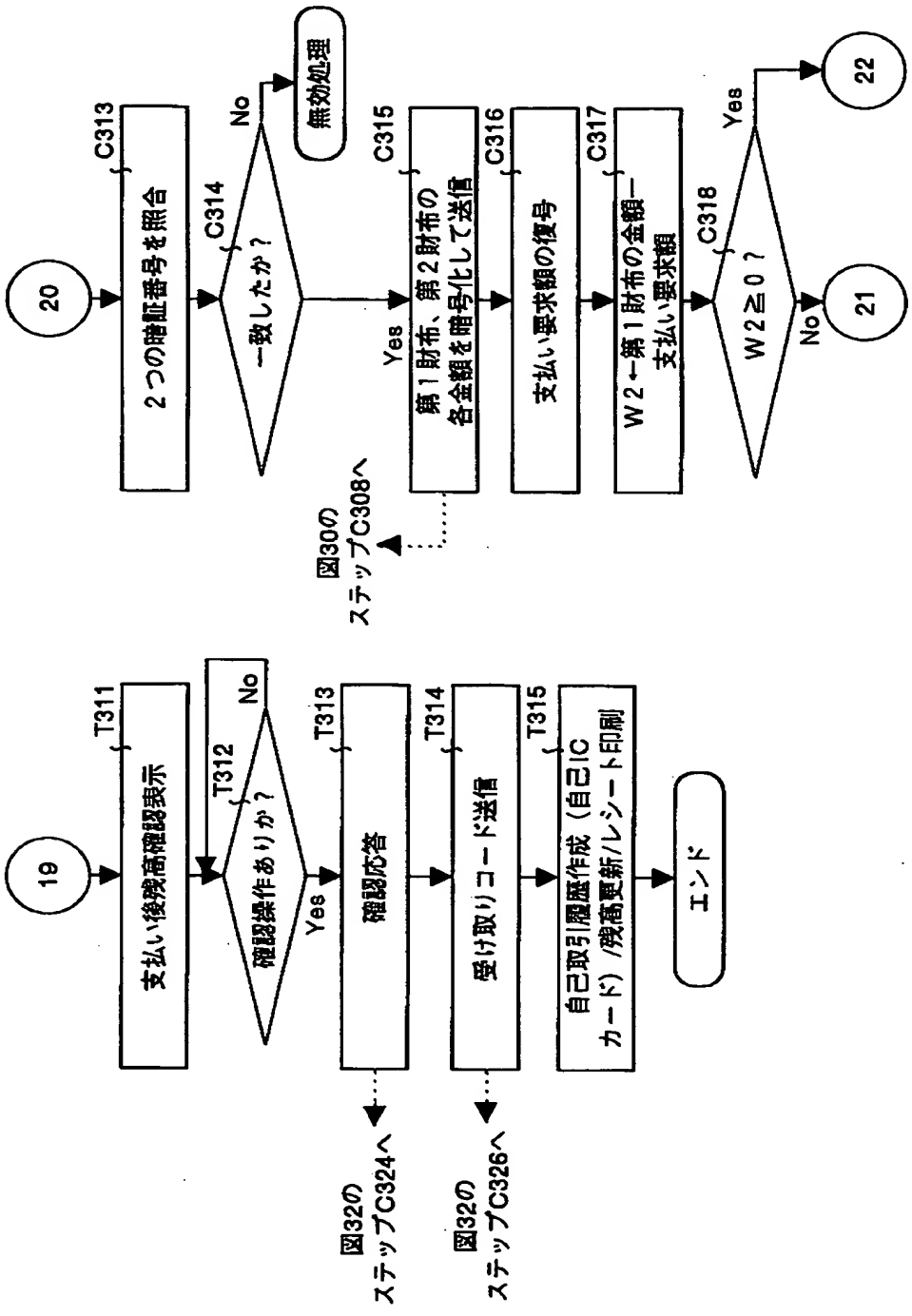
【図29】


引出装置2側処理
T301
取引金額入力/暗証番号入力/
カード挿入指示
T302
前処理用の処理
T303
金額入力/暗証番号入力
T304
機械ID，領域ID（第1財布），
支払いコマンド送信
17
ICカード1側処理
C301
前処理
C302
コマンド受信
C303
受信コマンドは
領域IDを含むか？
No
Yes
エンド
C304
領域IDの領域読み取り
C305
機械IDは一致か？
No
Yes
C306
機械IDのアクセス権と受信
アクセスとが対応か？
No
Yes
無効処理
18

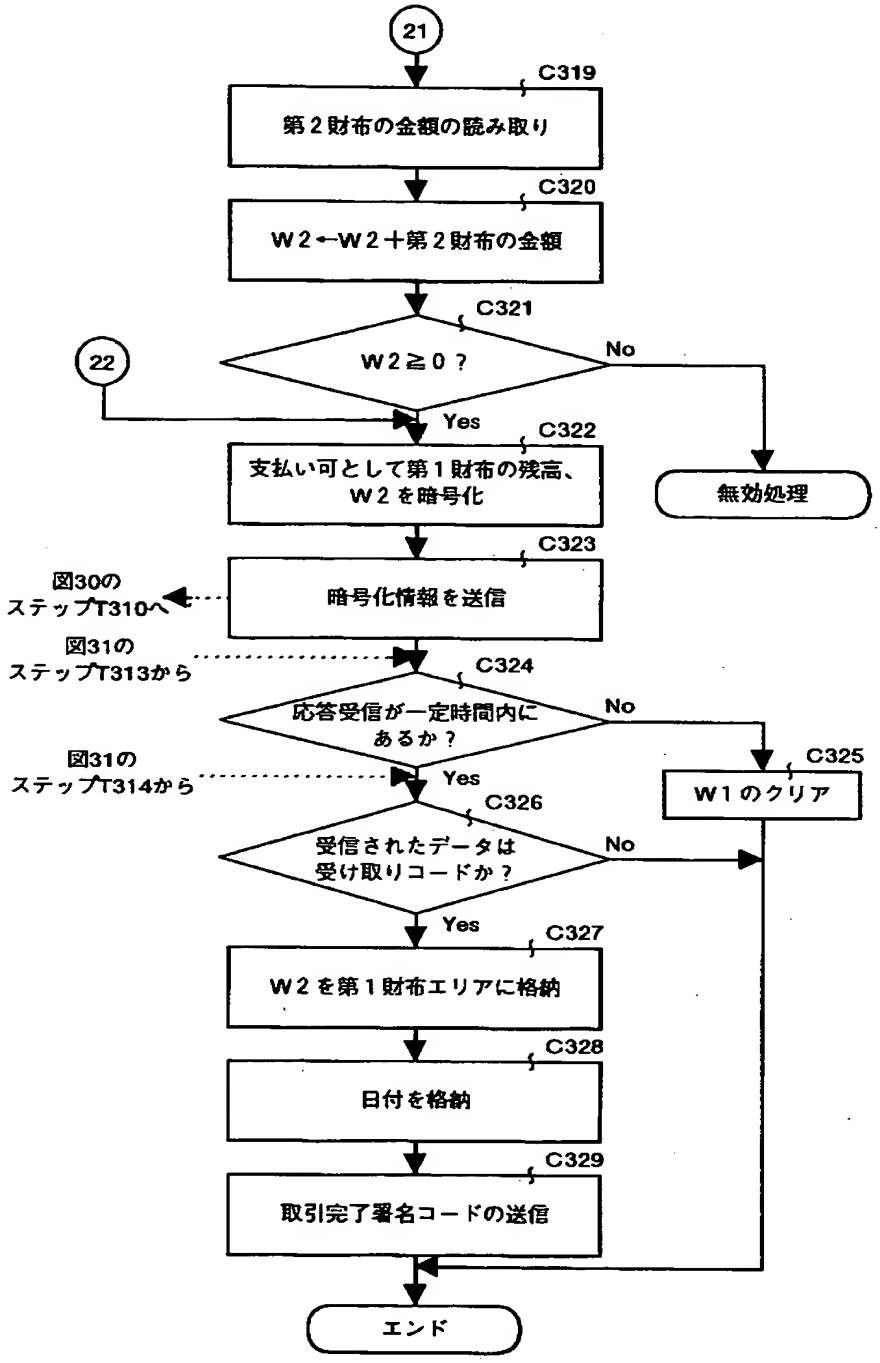
【図３０】


18
C307
領域は第１財布エリアか？
No
他モード
Yes
C308
要求は支払いか？
No
エンド
Yes
C309
暗証番号/支払い額要請
C310
暗証番号/支払い要求額受信
C311
暗証番号の復号
C312
第１財布の暗証番号を読み出す
20
17
T305
両情報あり判断
T306
両情報暗号化
T307
暗号化情報送信
T308
残高受信
T309
残高表示
T310
支払い可受信待ち
19
図31のステップC315から
図32のステップC323から

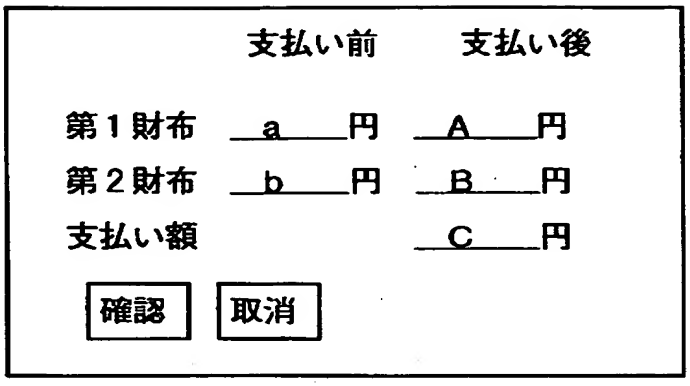
【図３１】


20
C313
２つの暗証番号を照合
C314
一致したか？
No
無効処理
Yes
C315
第１財布、第２財布の各金額を暗号化して送信
C316
支払い要求額の復号
C317
W２←第１財布の金額－支払い要求額
C318
W２≧０？
Yes
22
No
21
図30のステップC308へ
19
T311
支払い後残高確認表示
T312
確認操作ありか？
No
Yes
T313
確認応答
T314
受け取りコード送信
T315
自己取引履歴作成（自己ICカード）/残高更新/レシート印刷
エンド
図32のステップC324へ
図32のステップC326へ

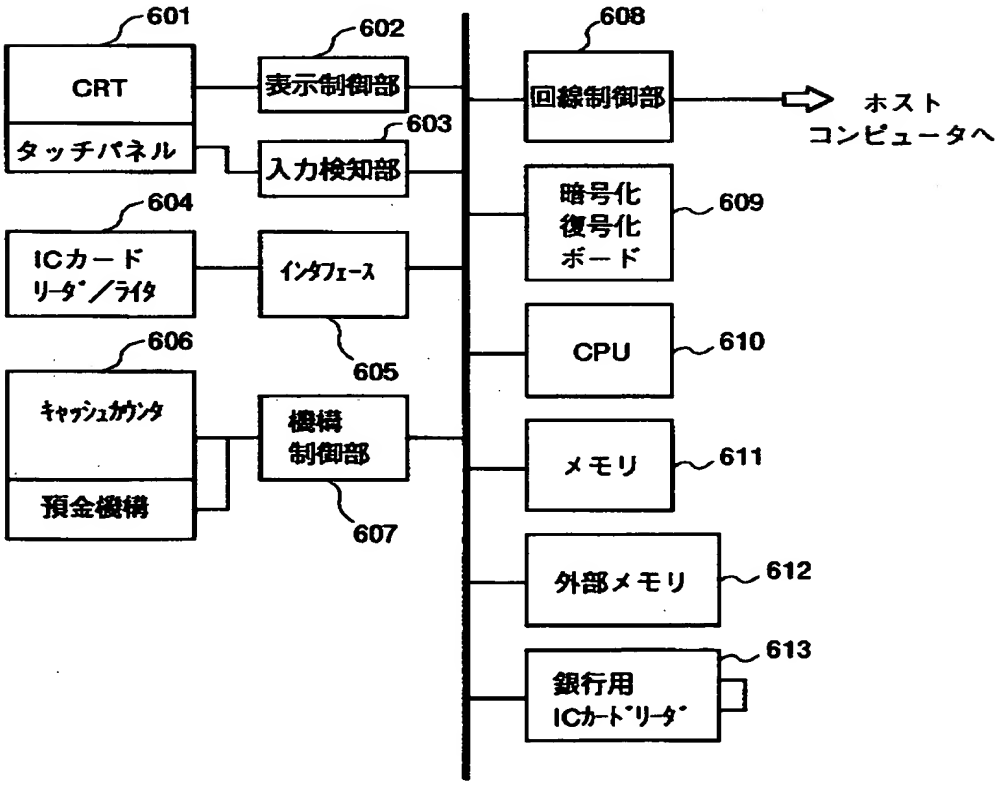
【図３２】


21
C319
第２財布の金額の読み取り
C320
W２←W２＋第２財布の金額
C321
22
W２≧０？
No
Yes
C322
支払い可として第１財布の残高、W２を暗号化
無効処理
C323
図30のステップT310へ
暗号化情報を送信
図31のステップT313から
C324
応答受信が一定時間内にあるか？
No
図31のステップT314から
Yes
C325
W１のクリア
C326
受信されたデータは受け取りコードか？
No
Yes
C327
W２を第１財布エリアに格納
C328
日付を格納
C329
取引完了署名コードの送信
エンド

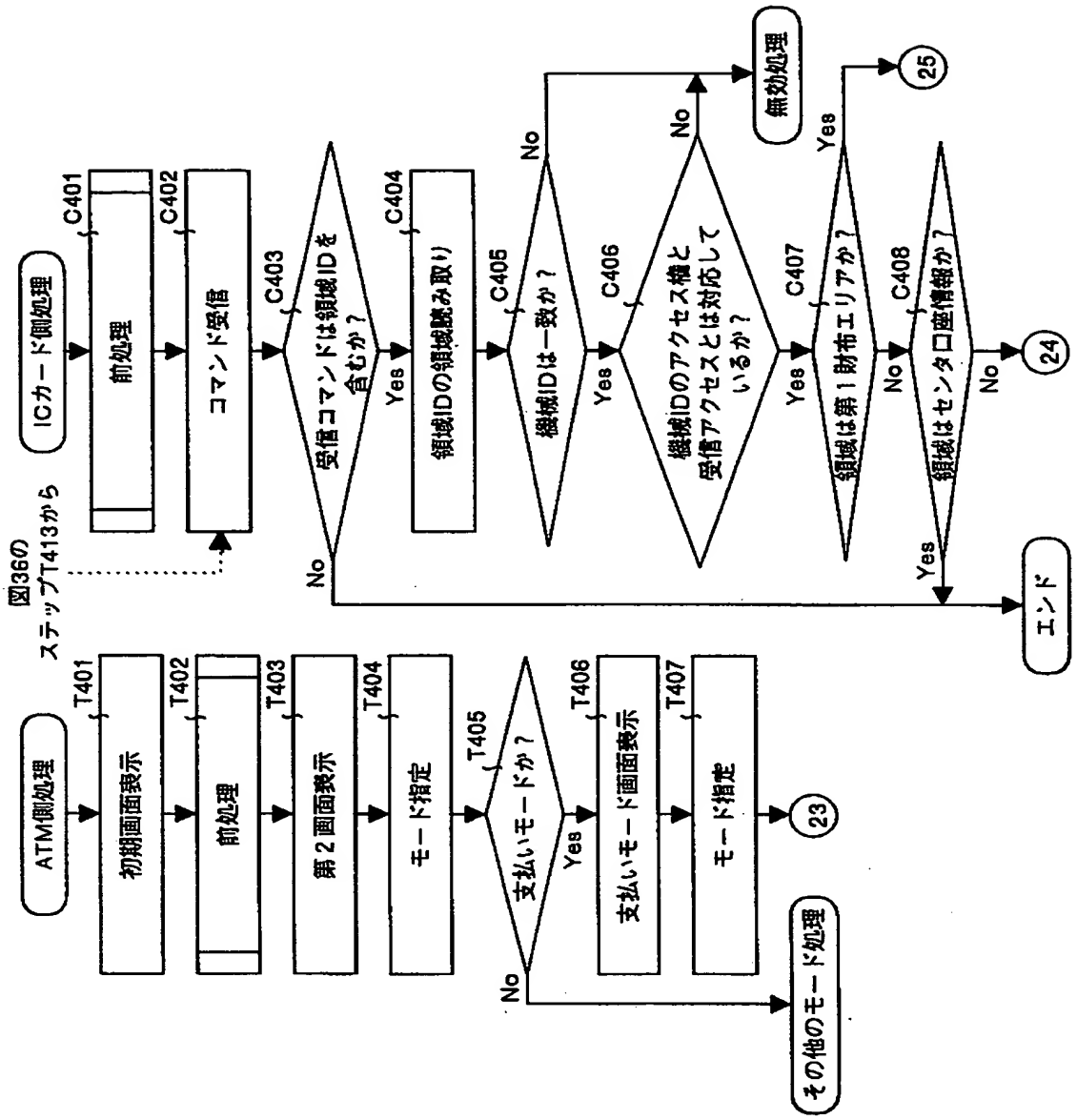
【図３３】


支払い前
支払い後
第１財布
a 円
A 円
第２財布
b 円
B 円
支払い額
C 円
確認
取消

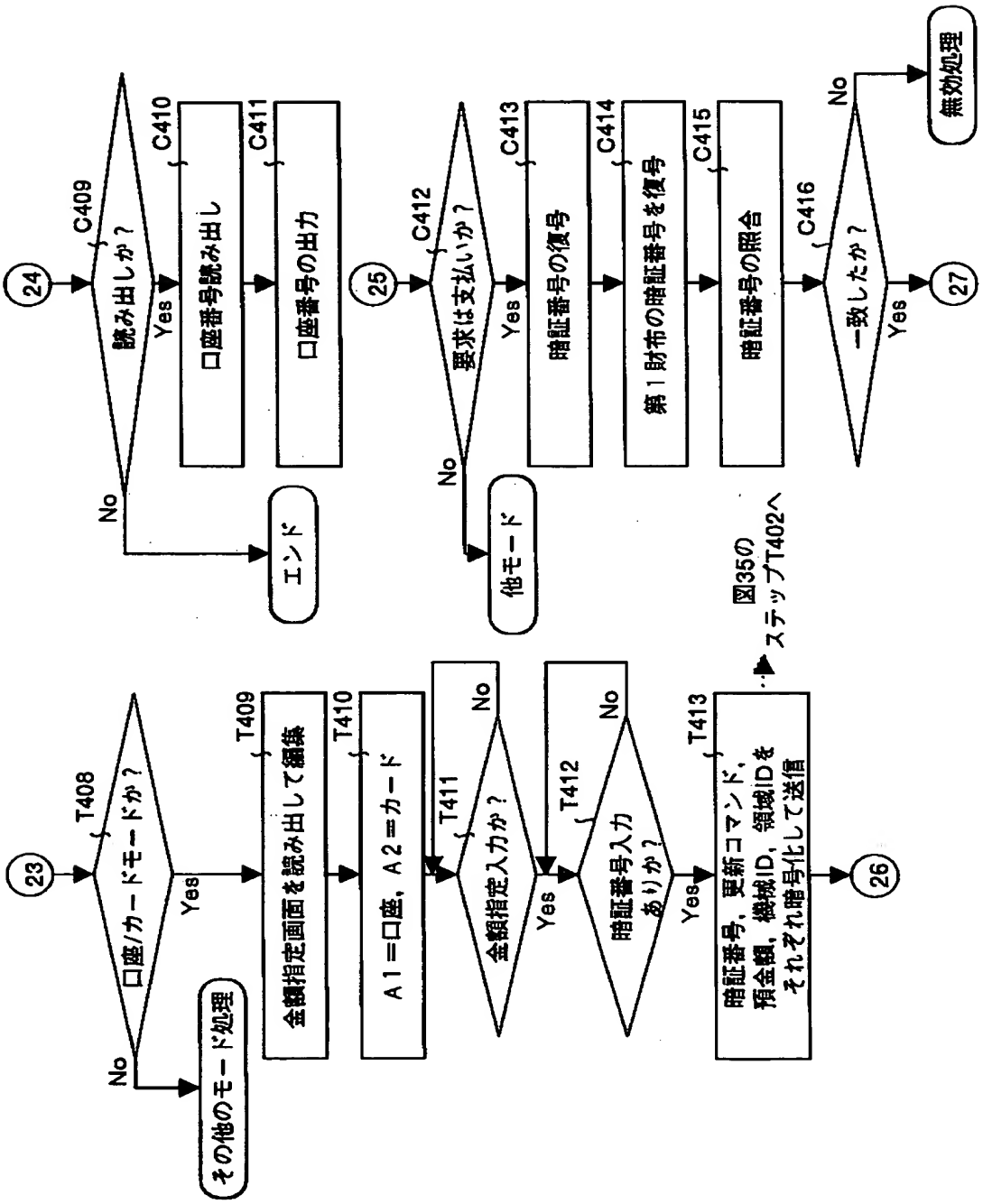
【図３４】


601
CRT
タッチパネル
602
表示制御部
603
入力検知部
604
ICカード
リーダ／ライタ
インタフェース
605
606
キャッシュカウンタ
預金機構
機構
制御部
607
608
回線制御部
ホスト
コンピュータへ
暗号化
復号化
ボード
609
CPU
610
メモリ
611
外部メモリ
612
613
銀行用
ICカードリーダ

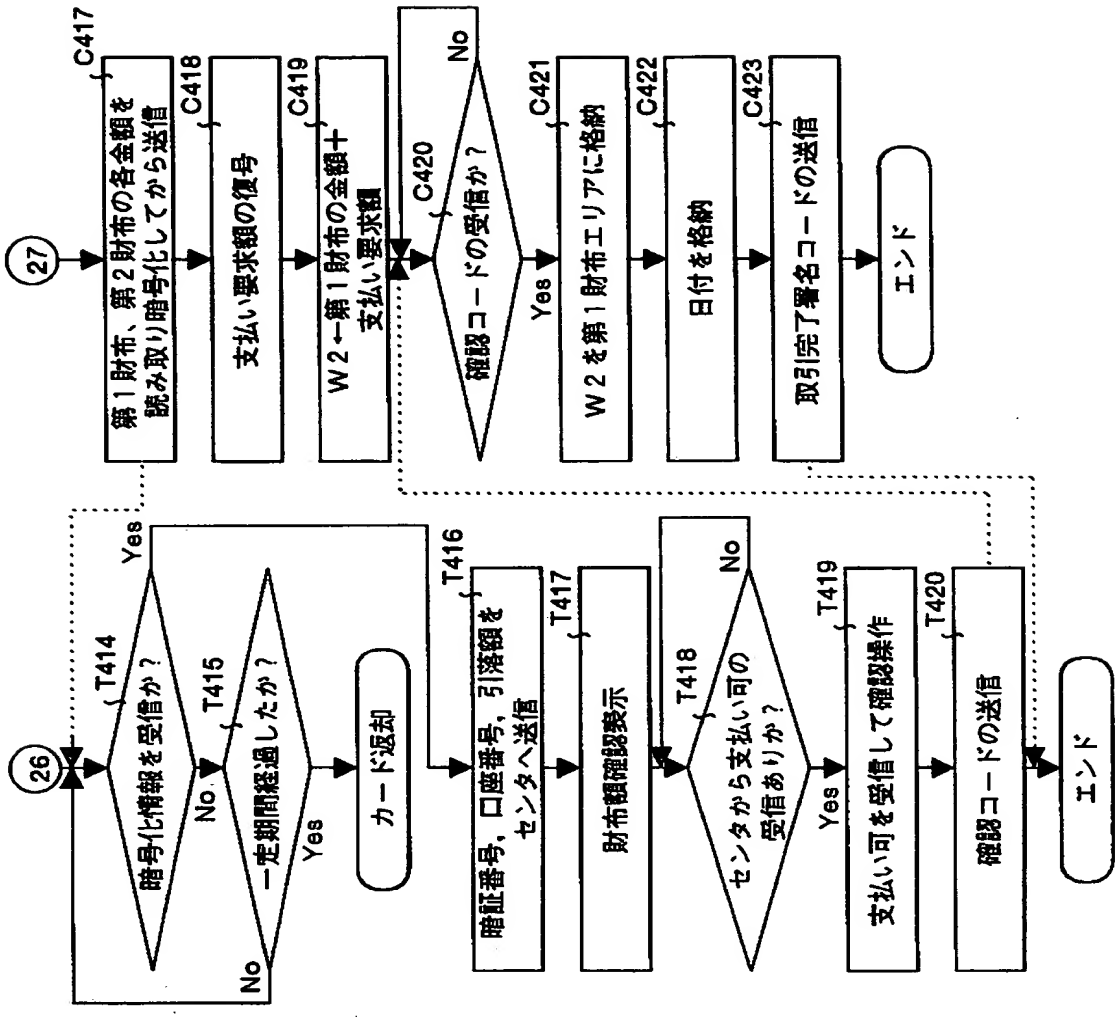
【図３５】


ATM側処理
初期画面表示
前処理
第２画面表示
モード指定
支払いモードか？
支払いモード画面表示
モード指定
その他のモード処理
T401
T402
T403
T404
T405
T406
T407
23
No
Yes
ICカード側処理
前処理
コマンド受信
受信コマンドは領域IDを含むか？
領域IDの領域読み取り
機械IDは一致か？
機械IDのアクセス権と受信アクセスとは対応しているか？
領域は第１財布エリアか？
領域はセンタ口座情報か？
無効処理
エンド
C401
C402
C403
C404
C405
C406
C407
C408
24
25
図36のステップT413から

【図３６】


(23)
T408
口座/カードモードか？
Yes
No
その他のモード処理
T409
金額指定画面を読み出して編集
T410
A1＝口座，A2＝カード
T411
金額指定入力か？
No
Yes
T412
暗証番号入力ありか？
No
Yes
T413
暗証番号，更新コマンド，預金額，機械ID，領域IDをそれぞれ暗号化して送信
(26)
図35のステップT402へ
(24)
C409
読み出しか？
Yes
No
C410
口座番号読み出し
C411
口座番号の出力
エンド
(25)
C412
要求は支払いか？
Yes
No
他モード
C413
暗証番号の復号
C414
第1財布の暗証番号を復号
C415
暗証番号の照合
C416
一致したか？
No
Yes
無効処理
(27)

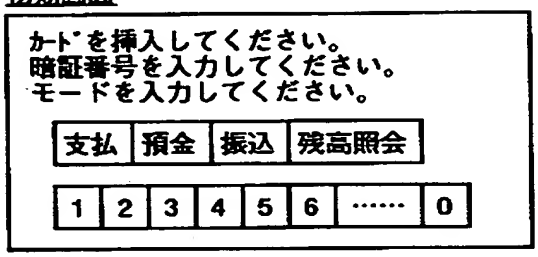
【図３７】


C417
第１財布、第２財布の各金額を読み取り暗号化してから送信
C418
支払い要求額の復号
C419
W２←第１財布の金額＋支払い要求額
C420
確認コードの受信か？
No
Yes
C421
W２を第１財布エリアに格納
C422
日付を格納
C423
取引完了署名コードの送信
エンド
27
26
T414
暗号化情報を受信か？
Yes
No
T415
一定期間経過したか？
No
Yes
カード返却
T416
暗証番号，口座番号，引落額をセンタへ送信
T417
財布額確認表示
T418
センタから支払い可の受信ありか？
No
Yes
T419
支払い可を受信して確認操作
T420
確認コードの送信
エンド

【図３８】

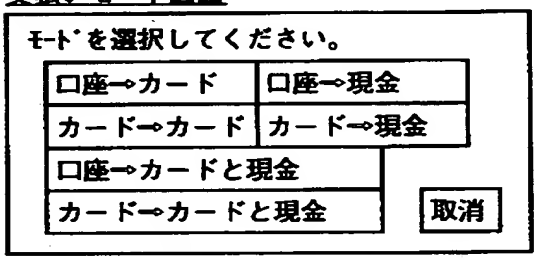
(a)

初期画面



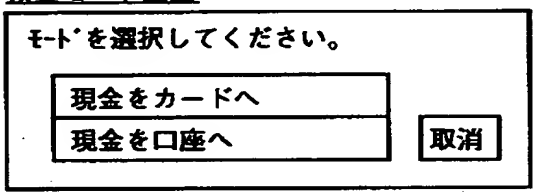
(b)

支払いモード画面



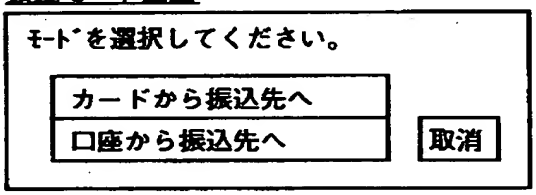
(c)

預金モード画面



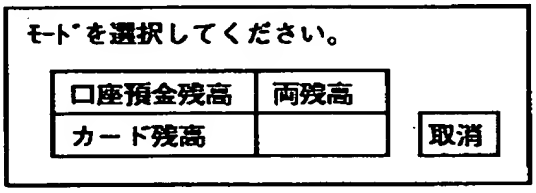
(d)

振込モード画面



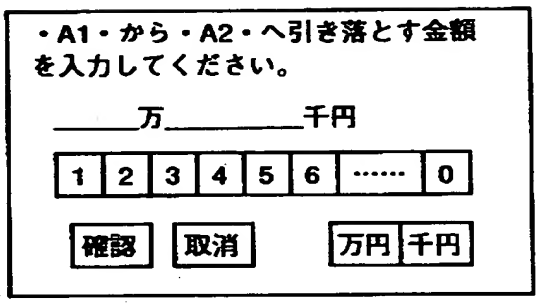
(e)

残高照会モード画面

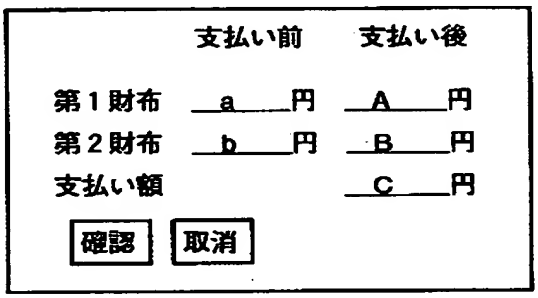


【図３９】

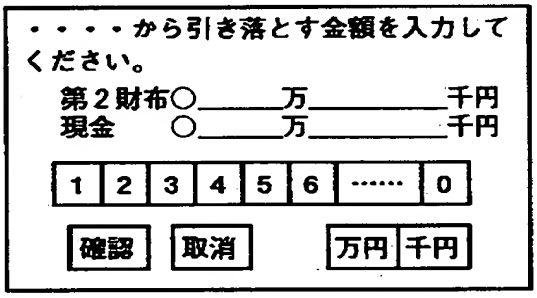
(a)


・A1・から・A2・へ引き落とす金額を入力してください。
＿＿＿万＿＿＿＿千円
1 2 3 4 5 6 …… 0
確認 取消 万円 千円

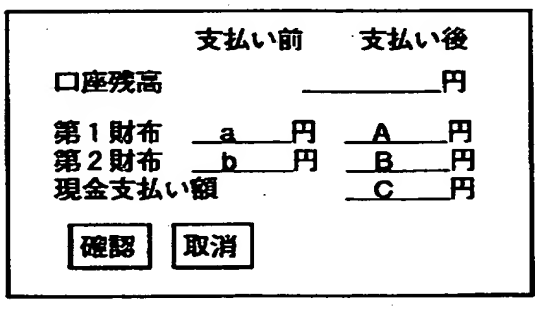
(b)


支払い前 支払い後
第１財布 a 円 A 円
第２財布 b 円 B 円
支払い額 C 円
確認 取消

(c)


・・・・から引き落とす金額を入力してください。
第２財布○＿＿＿万＿＿＿＿千円
現金 ○＿＿＿万＿＿＿＿千円
1 2 3 4 5 6 …… 0
確認 取消 万円 千円

(d)


支払い前 支払い後
口座残高 ＿＿＿＿円
第１財布 a 円 A 円
第２財布 b 円 B 円
現金支払い額 C 円
確認 取消

【書類名】　　要約書

【要約】

【課題】　セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることを課題とする。

【解決手段】　転送装置を用いたセキュリティの高い取引きの場合、暗証番号を用いた個人認証を通じてＩＣカードの第１財布（第１財布エリア１０６Ａ）から第２財布（第２財布エリア１０６Ｂ）への預金額の転送を行い、利用装置を用いたセキュリティの低い取引きの場合、個人認証を必要とせずに、ＩＣカードの第２財布で利用金額を利用する。

【選択図】　　図３

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【代理人】　申請人
【識別番号】　100089118
【住所又は居所】　東京都千代田区霞が関３丁目２番６号　東京倶楽部ビルディング　酒井国際特許事務所
【氏名又は名称】　酒井　宏明

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社